

Installieren und Aktualisieren von vRealize Automation

5. Oktober 2018

vRealize Automation 7.4



vmware®

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

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

Die VMware-Website enthält auch die neuesten Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

VMware, Inc.

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

VMware Global, Inc.

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

Inhalt

1	Installieren oder Aktualisieren von vRealize Automation	4
	vRealize Automation -Referenzarchitektur	4
	Empfehlungen für die anfängliche Bereitstellung und Konfiguration	4
	vRealize Automation -Bereitstellung	5
	Erwägungen zur Bereitstellung von vRealize Business for Cloud	7
	vRealize Automation -Skalierbarkeit	8
	vRealize Business for Cloud -Skalierbarkeit	11
	Erwägungen zur Konfiguration der Hochverfügbarkeit (HA, High Availability) von vRealize Automation	11
	Erwägungen zur Hochverfügbarkeit (HA, High Availability) von vRealize Business for Cloud	13
	vRealize Automation -Hardware-Spezifikationen und maximale Kapazitäten	14
	Anforderungen an die kleine Bereitstellungen von vRealize Automation	16
	Anforderungen an mittlere vRealize Automation -Bereitstellungen	21
	Anforderungen an große vRealize Automation -Bereitstellungen	27
	Bereitstellung von Daten für mehrere vRealize Automation -Datencenter	33
	Sichere Konfiguration von vRealize Automation	34
	Sichere Baseline für vRealize Automation – Übersicht	35
	Überprüfen der Integrität der Installationsmedien	36
	Härtung der Softwareinfrastruktur für VMware -Systeme	36
	Überprüfen der installierten Software	38
	Empfehlungen und Patches für die Sicherheit von VMware	38
	Sichere Konfiguration	39
	Konfigurieren der Hostnetzwerksicherheit	73
	Überwachung und Protokollierung	89
	Installieren von vRealize Automation	90
	Überblick über die vRealize Automation -Installation	90
	Vorbereitung für die Installation von vRealize Automation	99
	Bereitstellen der vRealize Automation -Appliance	116
	Installieren von vRealize Automation mit dem Installationsassistenten	123
	Die vRealize Automation -Standard-Installationsschnittstellen	150
	Automatische Installation von vRealize Automation	234
	vRealize Automation -Aufgaben nach der Installation	242
	Fehlerbehebung bei einer vRealize Automation -Installation	261
	Aktualisieren von vRealize Automation	290
	Upgrade von vRealize Automation 7.1 oder höher auf 7.4	293
	Upgrade von vRealize Automation 6.2.5 auf 7.4	367
	Migrieren auf vRealize Automation 7.4	457

Installieren oder Aktualisieren von vRealize Automation

1

Sie können vRealize Automation erstmalig installieren oder Ihre aktuelle Umgebung auf die neueste Version aktualisieren.

Dieses Kapitel enthält die folgenden Themen:

- [vRealize Automation-Referenzarchitektur](#)
- [Sichere Konfiguration von vRealize Automation](#)
- [Installieren von vRealize Automation](#)
- [Aktualisieren von vRealize Automation](#)

vRealize Automation -Referenzarchitektur

Referenzarchitektur beschreibt die Struktur und Konfiguration von typischen vRealize Automation-Bereitstellungen. Zudem bietet sie Informationen zur Hochverfügbarkeit, Skalierbarkeit und zu Bereitstellungsprofilen.

Referenzarchitektur beinhaltet Informationen zu den folgenden Komponenten:

- VMware vRealize Automation
- VMware vRealize Business for Cloud

Informationen zu Softwareanforderungen, Installationen und unterstützten Plattformen finden Sie in der jeweiligen Produktdokumentation.

Empfehlungen für die anfängliche Bereitstellung und Konfiguration

Stellen Sie alle VMware vRealize Automation-Komponenten gemäß den Empfehlungen von VMware bereit und konfigurieren Sie sie.

Stellen Sie sicher, dass die Zeitzone von vRealize Automation, vRealize Business for Cloud und vRealize Orchestrator identisch ist und die Systemuhren synchronisiert sind.

Installieren Sie vRealize Automation, vRealize Business for Cloud und vRealize Orchestrator auf demselben Verwaltungscluster. Stellen Sie Maschinen für einen vom Verwaltungscluster getrennten Cluster bereit, sodass Benutzerarbeitslasten und Serverarbeitslasten isoliert werden können.

Stellen Sie Proxy-Agents in dem Datacenter bereit, in dem auch der Endpoint, mit dem die Agents kommunizieren, enthalten ist. VMware rät von der Platzierung von DEM-Workern in Remote-Datenzentern ab, es sei denn, dies ist für eine bestimmte auf einem Anwendungsfall basierte Workflow-Fähigkeit ausdrücklich erforderlich. Alle Komponenten, außer Proxy-Agents und DEM-Worker, müssen in demselben oder denselben Datacentern innerhalb eines Metropolitan Area Network bereitgestellt werden. Die Latenz muss 5 Millisekunden unterschreiten und die Bandbreite zwischen den Datacentern und dem Metropolitan Area Network darf nicht weniger als 1GB/s sein.

Weitere Informationen einschließlich Angaben zur verfügbaren Unterstützung finden Sie im VMware Knowledgebase-Artikel *Installing the VMware vRealize Automation on a distributed multi-site instance* (Installieren von VMware vRealize Automation auf einer verteilten Instanz mit mehreren Sites) unter http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2134842.

vRealize Automation -Bereitstellung

Verwenden Sie die VMware-Ressourcenempfehlungen als Startpunkt für die Planung der vRealize Automation-Bereitstellung.

Fahren Sie nach der Durchführung der ersten Tests und der Bereitstellung in der Produktionsumgebung mit der Leistungsüberwachung fort und weisen Sie ggf. zusätzliche Ressourcen zu (siehe [vRealize Automation-Skalierbarkeit](#)).

Authentifizierung

Beim Konfigurieren von vRealize Automation können Sie den Standard-Connector für die Verzeichnisverwaltung für die Benutzerauthentifizierung verwenden oder einen bereits bestehenden SAML-basierten Identitätsanbieter angeben, um die einmalige Anmeldung zu unterstützen.

Wenn die Zwei-Faktor-Authentifizierung erforderlich ist, unterstützt vRealize Automation die Integration mit RSA SecurID. Wenn dieser Integrationspunkt konfiguriert ist, werden die Benutzer zur Angabe Ihrer Benutzer-ID und der Kennung aufgefordert.

Erwägungen zu Lastausgleichsdiensten

Verwenden Sie die Methode für die letzte Reaktionszeit oder die Round-Robin-Methode, um den Datenverkehr auf die vRealize Automation-Appliances und Infrastruktur-Webserver zu verteilen. Aktivieren Sie Sitzungsaffinität oder die Funktion für Sticky-Sitzungen, um nachfolgende Anforderungen aus jeder einzelnen Sitzung an denselben Webserver im Lastausgleichsdienst-Pool umzuleiten.

Sie können einen Lastausgleichsdienst verwenden, um Failover für den Manager Service zu verwalten. Verwenden Sie jedoch keinen Lastausgleichs-Algorithmus, da immer nur jeweils ein Manager Service aktiv ist. Verwenden Sie auch keine Sitzungsaffinität beim Verwalten eines Failovers mit einem Lastausgleichsdienst.

Verwenden Sie die Ports 443 und 8444 für den Lastausgleich der vRealize Automation-Appliance. Für die Infrastruktur-Website und den Infrastruktur-Manager Service sollte der Lastausgleich nur für Port 443 durchgeführt werden.

Obwohl Sie auch andere Lastausgleichsdienste verwenden können, wurden NSX, F5 BIG-IP-Hardware und F5 BIG-IP Virtual Edition getestet und deren Verwendung wird empfohlen.

Weitere Informationen zum Konfigurieren von Lastausgleichsdiensten finden Sie in der vRealize Automation-Dokumentation.

Datenbankbereitstellung

vRealize Automation gruppiert die Appliance-Datenbank in 7.0 und höheren Versionen automatisch als Cluster. Alle neuen Bereitstellungen von 7.0 und höheren Versionen müssen die interne Appliance-Datenbank verwenden. Bei vRealize Automation-Instanzen, die auf 7.1 oder höher aktualisiert werden, müssen die externen Datenbanken in der Appliance-Datenbank zusammengeführt werden. Weitere Informationen zum Upgrade-Prozess finden Sie in der Produktdokumentation zu vRealize Automation.

Verwenden Sie für Produktbereitstellungen von Infrastruktur-Komponenten einen dedizierten Datenbankserver als Host für die Microsoft SQL Server (MSSQL)-Datenbanken. vRealize Automation benötigt Maschinen, die mit dem Datenbankserver kommunizieren, der zur Verwendung von Microsoft Distributed Transaction Coordinator (MSDTC) konfiguriert ist. Standardmäßig benötigt MSDTC Port 135 und Ports 1024 bis 65535.

Weitere Informationen zum Ändern der standardmäßigen MSDTC-Ports finden Sie im Microsoft Knowledgebase-Artikel über die Konfiguration von Microsoft Distributed Transaction Coordinator (DTC) für eine Firewall unter <https://support.microsoft.com/de-de/kb/250367>

Der IaaS Manager Service-Host muss den NetBIOS-Namen des IaaS-SQL-Server-Datenbankhosts auflösen können. Wenn er den NetBIOS-Namen nicht auflösen kann, fügen Sie der Datei `/etc/hosts` der Manager Service-Maschine den NetBIOS-Namen des SQL-Servers hinzu und starten Sie den Manager Service neu.

vRealize Automation unterstützt SQL AlwaysON-Gruppen nur mit Microsoft SQL Server 2016. Bei der Installation von SQL Server 2016 muss die Datenbank im 100-Modus erstellt werden. Verwenden Sie bei einer älteren Version von Microsoft SQL-Server eine Failover-Cluster-Instanz mit freigegebenen Festplatten. Weitere Informationen zur Konfiguration von SQL AlwaysOn-Gruppen mit MSDTC finden Sie in <https://msdn.microsoft.com/de-de/library/ms366279.aspx>.

Konfiguration der Datenerfassung

Die Standardeinstellungen für die Datenerfassung sind ein guter Startpunkt für die meisten Implementierungen. Fahren Sie nach der Bereitstellung in der Produktionsumgebung mit der Leistungsüberwachung für die Datenerfassung fort, um herauszufinden, ob Anpassungen vorgenommen werden müssen.

Proxy-Agents

Um die größtmögliche Leistung zu erzielen, stellen Sie Agents im selben Datacenter wie die Endpoints bereit, denen sie zugeordnet sind. Sie können zusätzliche Agents installieren, um den Durchsatz und die Parallelität des Systems zu erhöhen. Verteilte Bereitstellungen können über mehrere Agent-Server verfügen, die auf der ganzen Welt verteilt sind.

Wenn Agents in demselben Datacenter wie ihre zugeordneten Endpoints installiert sind, können Sie eine Erhöhung der Datenerfassungsleistung von durchschnittlich 200 Prozent beobachten. Die gemessene Erfassungszeit umfasst nur die Zeit für die Übertragung der Daten zwischen dem Proxy-Agent und dem Manager Service. Nicht enthalten ist die Zeit, die der Manager Service benötigt, um die Daten zu verarbeiten.

Beispiel: Sie stellen das Produkt derzeit in einem Datacenter in Palo Alto bereit und haben vSphere-Endpoints in Palo Alto, Boston und London. In dieser Konfiguration werden die vSphere-Proxy-Agents in Palo Alto, Boston und London für ihre jeweiligen Endpoints bereitgestellt. Wenn Agents stattdessen nur in Palo Alto bereitgestellt werden, wird möglicherweise für Boston und London eine Steigerung der Datenerfassungszeit um 200 Prozent angezeigt.

Konfiguration von Distributed Execution Manager

Im Allgemeinen sollten die DEM (Distributed Execution Manager)-Instanzen so nah wie möglich am Model Manager-Host platziert werden. Die Netzwerkverbindung zwischen der DEM Orchestrator-Instanz und dem Model Manager muss immer sehr stabil sein. Standardmäßig positioniert das Installationsprogramm DEM-Orchestratoren neben dem Manager Service. Erstellen Sie in Ihrem primären Datacenter zwei DEM Orchestrator-Instanzen, eine für Failover und zwei DEM Worker-Instanzen.

Wenn eine DEM Worker-Instanz einen auf einen Standort bezogenen Workflow ausführen muss, installieren Sie die Instanz an diesem Standort.

Weisen Sie den jeweiligen Workflows und DEM-Instanzen Fähigkeiten zu, sodass diese Workflows immer von DEM-Instanzen am richtigen Standort ausgeführt werden. Informationen zum Zuweisen von Fähigkeiten zu Workflows und DEM-Instanzen unter Verwendung der vRealize Automation-Designerkonsole finden Sie in der Dokumentation zur Erweiterbarkeit von vRealize Automation.

Um eine maximale Leistung zu erzielen, installieren Sie die DEM-Instanzen und Agents auf getrennten Maschinen. Weitere Informationen zum Installieren von vRealize Automation-Agents finden Sie unter [Installieren von Agents](#).

vRealize Orchestrator

Verwenden Sie die interne vRealize Orchestrator-Instanz für alle neuen Bereitstellungen. Bei alten Bereitstellungen können Sie bei Bedarf eine externe vRealize Orchestrator einsetzen. Weitere Informationen zum Verfahren zur Erweiterung des Speichers, der der internen vRealize Orchestrator-Instanz zugewiesen ist, finden Sie unter https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109.

Prüfen und implementieren Sie für maximale Leistung die Konfigurationsrichtlinien im *Handbuch für das vRealize Orchestrator Coding-Design*, bevor Sie vRealize Orchestrator-Inhalte in Produktionsbereitstellungen importieren.

Erwägungen zur Bereitstellung von vRealize Business for Cloud

Stellen Sie vRealize Business for Cloud, früher als vRealize Business Standard Edition bekannt, gemäß den VMware-Richtlinien bereit.

Erwägungen zu Lastausgleichsdiensten

Lastausgleich wird für Verbindungen zur Datenerfassung nicht unterstützt. Weitere Informationen finden Sie unter [vRealize Automation-Skalierbarkeit](#). Für Benutzeroberflächen- und API-Client-Verbindungen der vRealize Business for Cloud-Appliance können Sie den vRealize Automation-Lastausgleichsdienst verwenden.

vRealize Automation -Skalierbarkeit

Ziehen Sie beim Konfigurieren Ihres vRealize Automation-Systems alle zutreffenden Skalierbarkeitsfaktoren in Betracht.

Benutzer

Die vRealize Automation-Appliance ist für die Synchronisierung von weniger als 100.000 Benutzern konfiguriert. Wenn Ihr System mehr Benutzer enthält, müssen Sie der Verzeichnisverwaltung von vRealize Automation möglicherweise mehr Speicher hinzufügen. Weitere Informationen zum Hinzufügen von Speicher zur Verzeichnisverwaltung finden Sie unter [Hinzufügen von Speicher zur Verzeichnisverwaltung](#).

Skalierbarkeit für gleichzeitige Bereitstellungen

Standardmäßig verarbeitet vRealize Automation nur acht gleichzeitige Bereitstellungen pro Endpoint. Informationen zum Erhöhen dieses Grenzwerts finden Sie unter [Konfigurieren der gleichzeitigen Bereitstellung von Maschinen](#).

VMware empfiehlt, dass alle Bereitstellungen mit mindestens zwei DEM Worker-Instanzen beginnen sollten. In Version 6.x kann jede DEM Worker-Instanz 15 Workflows gleichzeitig verarbeiten. Diese Anzahl wurde für vRealize Automation 7.0 und höher auf 30 erhöht.

Wenn Maschinen mit Workflow-Stubs angepasst wurden, sollten Sie pro 20 gleichzeitig bereitzustellenden Maschinen über 1 DEM Worker-Instanz verfügen. Beispiel: Ein System, das 100 gleichzeitige Bereitstellungen unterstützt, sollte mindestens über 5 DEM Worker-Instanzen verfügen.

Weitere Informationen zu DEM Worker-Instanzen und zur Skalierbarkeit finden Sie unter [Distributed Execution Manager-Leistungsanalyse und Tuning](#).

Skalierbarkeit bei der Datenerfassung

Die Fertigstellungszeit für die Datenerfassung hängt unter anderem von der Kapazität der Computing-Ressource, der Anzahl der Maschinen auf der Computing-Ressource oder dem Endpoint, dem aktuellen System und der Netzwerklast ab. Die Skalen für die Leistung variieren je nach Typ der Datenerfassung.

Für jeden Datenerfassungstyp gilt ein Standardintervall, das Sie überschreiben oder ändern können. Infrastrukturadministratoren können die Datenerfassung für Infrastruktur-Quell-Endpoints manuell initiieren. Fabric-Administratoren können die Datenerfassung für Computing-Ressourcen manuell initiieren. Die folgenden Werte sind die Standardintervalle für die Datenerfassung.

Tabelle 1-1. Standardintervalle für die Datenerfassung

Datenerfassungstyp	Standardintervall
Bestandsliste	Alle 24 Stunden (täglich)
Zustand	Alle 15 Minuten
Leistung	Alle 24 Stunden (täglich)

Leistungsanalyse und Tuning

Da die Anzahl der Ressourcen für die Datenerfassung zunimmt, können die Datenerfassungszeiten länger als das Intervall zwischen den Datenerfassungsintervallen sein, besonders bei der Erfassung von Zustandsdaten. Um zu festzustellen, ob die Datenerfassung für eine Computing-Ressource oder einen Endpoint rechtzeitig abgeschlossen oder in die Warteschlange gestellt wird, navigieren Sie zur Seite „Datenerfassung“. Bei Abschluss der Datenerfassung kann der Feldwert „Zuletzt abgeschlossen“ den Zustand `In Warteschlange` oder `Vorgang läuft` anstelle eines Zeitstempels anzeigen. Wenn dieses Problem auftritt, können Sie das Intervall zwischen Datenerfassungen erhöhen, um die Datenerfassungsfrequenz zu verringern.

Alternativ dazu können Sie den Grenzwert für die gleichzeitige Datenerfassung pro Agent erhöhen. Standardmäßig beschränkt vRealize Automation die Anzahl der gleichzeitigen Datenerfassungen auf zwei pro Agent und stellt Anforderungen in die Warteschlange, die diesen Grenzwert übersteigen. Durch diese Beschränkung können Datenerfassungsaktivitäten schnell beendet werden, ohne sich negativ auf die Gesamtleistung auszuwirken. Sie können den Grenzwert erhöhen, um die Vorteile der gleichzeitigen Datenerfassung zu nutzen. Bedenken Sie bei dieser Entscheidung jedoch möglicherweise negative Auswirkungen auf die Gesamtleistung.

Wenn Sie den für vRealize Automation konfigurierten Grenzwert pro Agent erhöhen, möchten Sie vielleicht auch einen oder mehrere dieser Zeitüberschreitungsintervalle erhöhen. Weitere Informationen zum Konfigurieren der gleichzeitigen Datenerfassung und zu Zeitüberschreitungsintervallen finden Sie in der Dokumentation zur vRealize Automation-Systemverwaltung. Die Manager Service-Datenerfassung ist CPU-intensiv. Das Erhöhen der Verarbeitungsleistung des Manager Service-Hosts kann die Zeit verkürzen, die für die gesamte Datenerfassung nötig ist.

Besonders die Datenerfassung für Amazon Elastic Compute Cloud (Amazon AWS) kann sehr CPU-intensiv sein, vor allem, wenn Ihr System Daten aus mehreren Regionen gleichzeitig erfasst und wenn die Daten vorher nicht in diesen Regionen erfasst wurden. Dieser Datenerfassungstyp kann zu einem umfassenden Leistungsabfall der Website führen. Verringern Sie die Frequenz der Erfassung von Amazon AWS-Bestandslistendaten, wenn sich dies merklich auf die Leistung auswirkt.

Skalierbarkeit der Workflow-Verarbeitung

Die durchschnittliche Workflow-Verarbeitungszeit (vom Starten der Verarbeitung des Workflows durch DEM Orchestrator bis zum Beenden der Ausführung) erhöht sich mit der Anzahl der gleichzeitigen Workflows. Das Workflow-Volumen stellt die Anzahl der vRealize Automation-Aktivitäten dar, einschließlich Maschinenanforderungen und einige Datenerfassungsaktivitäten.

Konfigurieren des Manager Service für große Datenmengen

Wenn Sie voraussichtlich einen VMware vSphere-Cluster mit sehr vielen Objekten, wie zum Beispiel mindestens 3000 virtuelle Maschinen, verwenden, legen Sie in der Manager Service-Konfigurationsdatei höhere Werte fest. Wenn Sie diese Einstellung nicht ändern, schlägt die Erfassung von umfangreichen Bestandslistendaten möglicherweise fehl.

Ändern Sie den Standardwert der Einstellungen `ProxyAgentServiceBinding` und `maxStringLength` in der Datei `ManagerService.exe.config`.

Verfahren

- 1 Öffnen Sie die Datei `ManagerService.exe.config` mit einem Texteditor.

Diese Datei befindet sich normalerweise im Verzeichnis `C:\Program Files (x86)\VMware\Server`.

- 2 Suchen Sie die Zeilen `binding name` und `readerQuotas` in der Datei.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">  
  <readerQuotas maxStringLength="13107200" />
```

Hinweis Verwechseln Sie diese beiden Zeilen nicht mit ähnlichen Zeilen, die die folgende Zeichenfolge enthalten: `binding name = "ProvisionServiceBinding"`.

- 3 Ersetzen Sie die den Attributen `maxReceivedMessageSize` und `maxStringLength` zugewiesenen Zahlenwerte mit einem größeren Wert.

Die optimale Größe richtet sich danach, mit wie vielen weiteren Objekten Sie zukünftig in Ihrem VMware vSphere-Cluster rechnen. Sie können den jeweiligen Wert beispielsweise mit einem Faktor von 10 für Testzwecke erhöhen.

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.
- 5 Starten Sie den Manager Service von vRealize Automation neu.

Distributed Execution Manager-Leistungsanalyse und Tuning

Sie können die Gesamtanzahl der laufenden und ausstehenden Workflows jederzeit auf der Seite „Distributed Execution Status“ anzeigen und die Seite „Workflow History“ verwenden, um festzustellen, wie lange die Ausführung eines vorhandenen Workflows dauert.

Wenn Sie über eine große Anzahl an ausstehenden Workflows verfügen oder die Fertigstellung von Workflows länger dauert, als erwartet, fügen Sie weitere Distributed Execution Manager (DEM) Worker-Instanzen hinzu, um die Workflows zu verarbeiten. Jede DEM Worker-Instanz kann 30 Workflows gleichzeitig verarbeiten. Überschüssige Workflows werden zwecks Ausführung in die Warteschlange gestellt.

Sie können Workflow-Zeitpläne anpassen, um die Anzahl der Workflows zu reduzieren, die gleichzeitig starten. Anstatt alle stündlich auszuführenden Workflows an den Stundenanfang zu legen, können Sie deren Ausführung zeitlich versetzt planen, um die Nutzung von DEM-Ressourcen zu vermeiden. Weitere Informationen zu Workflows finden Sie in der Dokumentation zur Erweiterbarkeit von vRealize Automation.

Einige Workflows, besonders bestimmte benutzerdefinierte Workflows, können sehr CPU-intensiv sein. Wenn die CPU-Last auf den DEM Worker-Maschinen hoch ist, sollten Sie die Verarbeitungsleistung der DEM-Maschine erhöhen oder Ihrer Umgebung weitere DEM-Maschinen hinzufügen.

vRealize Business for Cloud -Skalierbarkeit

Konfigurieren Sie Ihre vRealize Business for Cloud-Installation gemäß den VMware-Richtlinien für Skalierbarkeit.

vRealize Business for Cloud kann bis zu 20.000 virtuelle Maschinen auf zehn VMware vCenter Server-Instanzen skalieren. Bei der ersten Synchronisierung der Bestandslistendatenerfassung dauert es ungefähr drei Stunden, bis 20.000 virtuelle Maschinen in drei VMware vCenter Server-Instanzen synchronisiert sind. Die Synchronisierung von Statistiken aus VMware vCenter Server nimmt für 20.000 virtuelle Maschinen ungefähr eine Stunde in Anspruch. Der Kostenberechnungs-Job wird täglich ausgeführt und nimmt bei jeder Ausführung für 20.000 virtuelle Maschinen ungefähr zwei Stunden in Anspruch.

Hinweis In vRealize Business for Cloud 1.0 unterstützt die Standardkonfiguration der virtuellen Appliance bis zu 20.000 virtuelle Maschinen. Durch das Erhöhen der Grenzwerte für die virtuelle Appliance über das in der Standardkonfiguration festgelegte Maß hinaus wird die Anzahl der von der Appliance unterstützten virtuellen Maschinen nicht erhöht.

Erwägungen zur Konfiguration der Hochverfügbarkeit (HA, High Availability) von vRealize Automation

Wenn Sie maximale Systemrobustheit benötigen, konfigurieren Sie Ihr vRealize Automation-System gemäß den VMware-Richtlinien für Hochverfügbarkeit.

vRealize Automation -Appliance

Die vRealize Automation-Appliance unterstützt aktive-aktive Hochverfügbarkeit für alle Komponenten mit Ausnahme der Appliance-Datenbank. Ab Version 7.3 erfolgt das Datenbank-Failover automatisch, wenn drei Knoten bereitgestellt werden und zwischen zwei Knoten eine synchrone Replikation konfiguriert wurde. Wenn vRealize Automation-Appliance Datenbankfehler erkennt, setzt es einen geeigneten Datenbankserver als Master ein. Sie können die Appliance-Datenbank in der Verwaltungskonsole der virtuellen Appliance auf der Registerkarte **vRA-Einstellungen > Datenbank** überwachen und verwalten.

Um Hochverfügbarkeit für diese Appliances zu aktivieren, platzieren Sie sie unter einem Lastausgleichsdienst. Weitere Informationen finden Sie unter [Konfigurieren des Lastausgleichsdiensts](#). Ab Version 7.0 werden die Appliance-Datenbank und vRealize Orchestrator automatisch einem Cluster hinzugefügt und stehen zur Verwendung zur Verfügung.

vRealize Automation -Verzeichnisverwaltung

Jede vRealize Automation-Appliance enthält einen Connector, der die Benutzerauthentifizierung unterstützt, jedoch ist in der Regel nur ein Connector zum Ausführen der Verzeichnissynchronisierung konfiguriert. Es spielt keine Rolle, welchen Connector Sie als Synchronisierungs-Connector auswählen. Damit die Verzeichnisverwaltung mit Hochverfügbarkeit unterstützt wird, müssen Sie einen zweiten Connector konfigurieren, der Ihrer zweiten vRealize Automation-Appliance entspricht. Dieser verbindet sich mit Ihrem Identitätsanbieter und verweist auf dasselbe Active Directory. Fällt eine Appliance aus, wird bei dieser Konfiguration die Verwaltung der Benutzerauthentifizierung von der anderen Appliance übernommen.

In einer hochverfügbaren Umgebung müssen alle Knoten dieselbe Gruppe von Active Directories, Benutzern, Authentifizierungsmethoden usw. bedienen. Am einfachsten wird dies dadurch erreicht, dass der Identitätsanbieter zum Cluster heraufgestuft wird, indem der Lastausgleichsdienst-Host als der Identitätsanbieter-Host eingerichtet wird. Mit dieser Konfiguration werden alle Authentifizierungsanforderungen an den Lastausgleichsdienst gerichtet, der diese dann an einen der Connectors weiterleitet.

Weitere Informationen zum Konfigurieren der Verzeichnisverwaltung für Hochverfügbarkeit finden Sie unter [Configure Directories Management for High Availability](#).

Infrastruktur-Webserver

Die Infrastruktur-Webserver-Komponenten unterstützen alle die Aktiv/Aktiv-Hochverfügbarkeit. Um Hochverfügbarkeit für diese Komponenten zu aktivieren, platzieren Sie sie unter einem Lastausgleichsdienst.

Infrastruktur-Manager Service

Die Manager Service-Komponente unterstützt die Aktiv/Aktiv-Hochverfügbarkeit. Um Hochverfügbarkeit für diese Komponenten zu aktivieren, platzieren Sie zwei Manager Service-Instanzen unter einem Lastausgleichsdienst. In vRealize Automation 7.3 und neueren Versionen erfolgt das Failover automatisch.

Wenn der aktive Manager Service fehlschlägt, beenden Sie den Windows-Dienst, falls dieser nicht bereits unter dem Lastausgleichsdienst beendet wurde. Aktivieren Sie den passiven Manager Dienst und starten Sie den Windows-Dienst unter dem Lastausgleichsdienst neu. Siehe [Installieren der aktiven Manager Service-Komponente](#).

Agents

Agents unterstützen Aktiv/Aktiv-Hochverfügbarkeit. Weitere Informationen zum Konfigurieren von Agents für Hochverfügbarkeit finden Sie in der Dokumentation zur Konfiguration von vRealize Automation. Überprüfen Sie den Zieldienst auf Hochverfügbarkeit.

Distributed Execution Manager Worker

Ein unter der Worker-Rolle ausgeführter Distributed Execution Manager (DEM) unterstützt Aktiv/Aktiv-Hochverfügbarkeit. Wenn eine DEM Worker-Instanz fehlschlägt, erkennt DEM Orchestrator den Fehler und bricht alle Workflows ab, die von der DEM Worker-Instanz ausgeführt werden. Wenn die DEM Worker-Instanz erneut online geschaltet wird, erkennt sie, dass DEM Orchestrator die Workflows der Instanz abgebrochen hat und beendet deren Ausführung. Um das vorzeitige Abbrechen von Workflows zu vermeiden, behalten Sie den Offline-Modus einer DEM Worker-Instanz für mehrere Minuten bei, bevor Sie deren Workflows abbrechen.

Distributed Execution Manager Orchestrator

Die unter der Orchestrator-Rolle ausgeführten DEM-Instanzen unterstützen Aktiv/Aktiv-Hochverfügbarkeit. Beim Starten einer DEM Orchestrator-Instanz wird eine weitere laufende DEM Orchestrator-Instanz gesucht.

- Wenn keine laufende DEM Orchestrator-Instanz gefunden wird, wird diese Instanz als primäre DEM Orchestrator-Instanz ausgeführt.
- Wenn eine andere laufende DEM Orchestrator-Instanz gefunden wird, wird die andere primäre DEM Orchestrator-Instanz zwecks Erkennung eines Ausfalls überwacht.
- Bei Auftreten eines Ausfalls übernimmt diese Instanz die Rolle der primären Instanz.

Wenn eine vorherige primäre Instanz erneut online geschaltet wird, erkennt sie, dass eine andere DEM Orchestrator-Instanz ihre Rolle als primäre Instanz übernommen hat, woraufhin sie die Ausfallüberwachung der primären Orchestrator-Instanz übernimmt.

MSSQL-Datenbankserver für Infrastrukturkomponenten

vRealize Automation unterstützt SQL AlwaysON-Gruppen nur mit Microsoft SQL Server 2016. Bei der Installation von SQL Server 2016 muss die Datenbank im 100-Modus erstellt werden. Verwenden Sie bei einer älteren Version von Microsoft SQL-Server eine Failover-Cluster-Instanz mit freigegebenen Festplatten. Weitere Informationen zur Konfiguration von SQL AlwaysOn-Gruppen mit MSDTC finden Sie im Microsoft-Artikel <https://msdn.microsoft.com/en-us/library/ms366279.aspx>.

vRealize Orchestrator

Eine interne Hochverfügbarkeitsinstanz von vRealize Orchestrator wird als Teil der vRealize Automation-Appliance bereitgestellt.

Erwägungen zur Hochverfügbarkeit (HA, High Availability) von vRealize Business for Cloud

Verwenden Sie die VMware vSphere HA-Funktion für die vRealize Business for Cloud Edition-Appliance.

Informationen zur Konfiguration der VMware vSphere HA-Funktion auf dem VMware ESXi-Host finden Sie in der Dokumentation „vCenter Server und Hostverwaltung“.

vRealize Automation -Hardware-Spezifikationen und maximale Kapazitäten

Installieren Sie die erforderlichen Komponenten für Ihre Konfiguration und Ihren Kapazitätsbedarf auf jedem vRealize Automation-Serverprofil in Ihrer Umgebung.

Serverrolle	Komponenten	Spezifikationen der erforderlichen Hardware	Spezifikationen der empfohlenen Hardware
vRealize Automation-Appliance	vRealize Automation-Dienste, vRealize Orchestrator, vRealize Automation Appliance-Datenbank	CPU: 4 vCPU RAM: 18 GB (Siehe vRealize Automation-Skalierbarkeit .) Festplatte: 140 GB Netzwerk: 1 GB/s	Entspricht den Spezifikationen der erforderlichen Hardware.
Infrastruktur-Hauptserver	Website, Manager Service, DEM Orchestrator, DEM Worker, Proxy-Agent	CPU: 4 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	Entspricht den Spezifikationen der erforderlichen Hardware.
Infrastruktur-Webserver	Website	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s
Infrastruktur-Manager-Server	Manager Service, DEM Orchestrator	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s
Infrastruktur-Webserver/-Manager-Server	Infrastruktur-Webserver/-Manager-Server	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s
Infrastruktur-DEM-Server	(Mindestens eine) DEM Worker-Instanz	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s pro DEM Worker-Instanz	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s pro DEM Worker-Instanz
Infrastruktur-Agent-Server	(Mindestens ein) Proxy-Agent	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s

Serverrolle	Komponenten	Spezifikationen der erforderlichen Hardware	Spezifikationen der empfohlenen Hardware
MSSQL-Datenbankserver	Infrastruktur-Datenbank	CPU: 2 vCPU RAM: 8 GB Festplatte: 40 GB Netzwerk: 1 GB/s	CPU: 8 vCPU RAM: 16 GB Festplatte: 80 GB Netzwerk: 1 GB/s
vRealize Business for Cloud-Appliance	vRealize Business for Cloud-Appliance-Dienste vRealize Business for Cloud-Datenbankserver	CPU: 2 vCPU RAM: 4 GB Festplatte: 50 GB Netzwerk: 1 GB/s	Entspricht den Spezifikationen der erforderlichen Hardware.

Maximale empfohlene Kapazitäten für vRealize Automation

Die folgenden Maximalwerte für die Kapazität der Ressourcen gelten für das große Bereitstellungsprofil von vRealize Automation.

Tabelle 1-2. Maximale Ressourcenkapazitäten für vRealize Automation

Parameter	Maximalwert
Mandant	100
vSphere-Endpoints	20
Computing-Ressourcen	200
Verwaltete Maschinen	75.000
Höchstwert der gleichzeitigen Anforderung	
	Konstante 50
	Ausschläge 250
Höchstwert der Anforderungen pro Stunde	400
Business-Gruppen	3000 (mit 10 eindeutigen Benutzern pro Business-Gruppe, wobei kein Benutzer Mitglied von mehr als 50 Business-Gruppen ist)
Reservierungen	9.000 (mit drei Reservierungen pro Business-Gruppe)
Blueprints	
	nur CBP 6.000
	CBP + XaaS 8.000
Katalogelemente	
	für alle Mandanten 4.000
	für einen einzelnen Mandanten 6.000
Benutzer-/Gruppensynchronisierung mit standardmäßigen 18 GB Arbeitsspeicher	

Tabelle 1-2. Maximale Ressourcenkapazitäten für vRealize Automation (Fortsetzung)

Parameter	Maximalwert
Anzahl der Benutzer	95.027
Anzahl der Gruppen	20.403 (jede Gruppe umfasst vier Benutzer und eine Verschachtelungsebene)
Benutzer/Gruppe mit auf 30 GB erhöhtem Arbeitsspeicher	
Anzahl der Benutzer	100.000
Anzahl der Gruppen	750 (jede Gruppe umfasst 4.000 Benutzer und jeder Benutzer ist Mitglied in 30 Gruppen)

Anforderungen an die kleine Bereitstellungen von vRealize Automation

Eine kleine vRealize Automation-Bereitstellung umfasst Systeme mit 10.000 verwalteten Maschinen oder weniger mit den entsprechenden Maschinen, Lastausgleichsdiensten und Portkonfigurationen. Die kleine Bereitstellung dient als Startpunkt für eine vRealize Automation-Bereitstellung, die Sie nach und nach auf eine mittlere oder große Bereitstellung skalieren können.

Wenden Sie beim Bereitstellen von vRealize Automation das Verfahren zur Unternehmensbereitstellung an, um eine separate Infrastruktur-Website und Manager Service-Adresse bereitzustellen.

Support

Eine kleine Bereitstellung kann die folgenden Elemente unterstützen.

- 10.000 verwaltete Maschinen
- 500 Katalogelemente
- Gleichzeitige Bereitstellung von 10 Maschinen

Anforderungen

Eine kleine Bereitstellung muss mit den entsprechenden Komponenten konfiguriert werden.

- vRealize Automation-Appliance: vrava-1.ra.local
- Infrastruktur-Hauptserver: inf-1.ra.local.
- MSSQL-Datenbankserver: mssql.ra.local
- vRealize Business for Cloud-Appliance: vrb.ra.local

DNS-Einträge

DNS-Eintrag	Zeigt auf
vrava.ra.local	vrava-1.ra.local
web.ra.local	inf.ra.local
manager.ra.local	inf.ra.local

Zertifikate

Bei den in dieser Tabelle verwendeten Hostnamen handelt es sich nur um Beispiele.

Serverrolle	CN oder SAN
vRealize Automation-Appliance	SAN enthält vra.va.sqa.local und vra.va-1.sqa.local
Infrastruktur-Hauptserver	SAN enthält web.ra.local, managers.ra.local und inf-1.ra.local
vRealize Business for Cloud-Server	CN = vrb.ra.local

Ports

Benutzer benötigen Zugriff auf bestimmte Ports. Alle aufgelisteten Ports sind Standardports.

Serverrolle	Port
vRealize Automation-Appliance	443, 8444. Port 8444 ist für die VM-Remote-Konsole erforderlich. Port 8283 ist erforderlich, um auf das Control Center von vRealize Orchestrator zuzugreifen.

Neben den für Benutzer erforderlichen Ports benötigen Administratoren Zugriff auf bestimmte Ports.

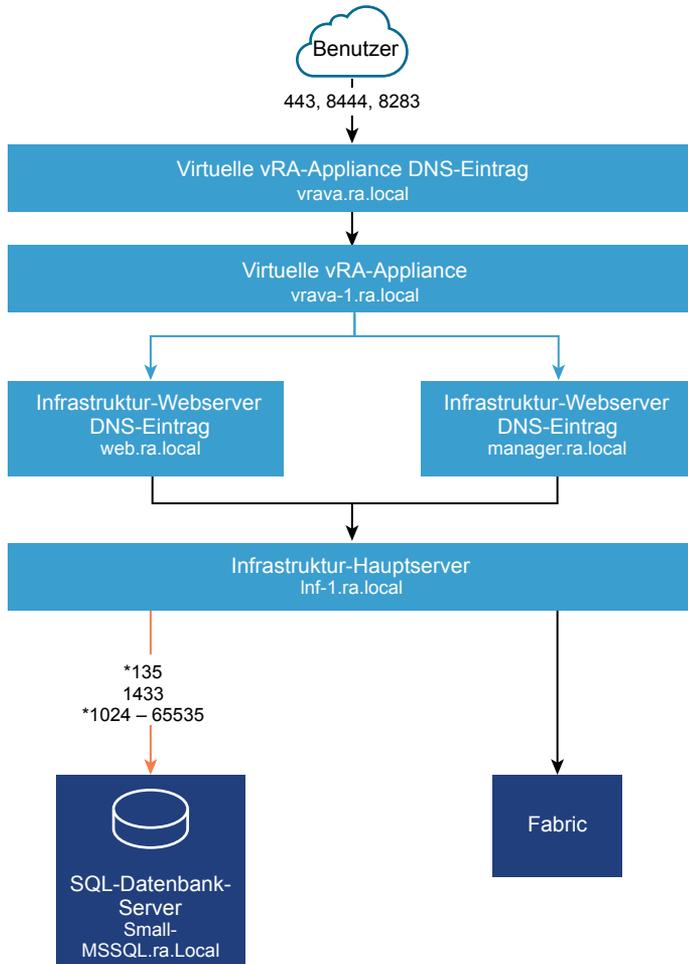
Serverrolle	Port
vRealize Automation-Appliance	5480, 8443. Port 8443 ist für die erweiterte Konfiguration der Identitätsverwaltung reserviert. VMware Identity Manager zu Active Directory: 389, 636, 3268, 3269 VMware Identity Manager zu Domänen-Controller: 88, 464, 135
vRealize Business for Cloud	5480

Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
vRealize Automation-Appliance	HTTPS: 443 Adapterkonfiguration: 8443 Remote-Konsolenproxy: 8444 SSH: 22 Verwaltungskonsole der virtuellen Appliance: 5480	LDAP: 389 LDAPS:636 VMware ESXi: 902 Infrastruktur-Hauptserver benötigt Zugriff auf Port 443 für den vSphere-Endpoint, um ein Ticket für die VMware Remote Console abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. Infrastruktur-Hauptserver: 443 Kerberos-Authentifizierung: 88 Computer-Objektkennwortverlängerung: 464
Infrastruktur-Hauptserver	HTTPS: 443 MSDTC: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	Virtuelle vRealize Automation-Appliance: 443, 5480 vSphere-Endpoint: 443 Infrastruktur-Hauptserver benötigt Zugriff auf Port 443 für den vSphere-Endpoint, um ein Ticket für die VMware Remote Console abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. MSSQL: 135, 1433, 1024 - 65535 MSDTC: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .

Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
MSSQL-Datenbankserver	MSSQL: 1433 MSDTC: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	Infrastruktur-Hauptserver: 135, 1024 bis 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung . MSDTC: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .
vRealize Business for Cloud-Appliance	HTTPS: 443 SSH: 22 Verwaltungskonsole der virtuellen Appliance: 5480	Virtuelle vRealize Automation-Appliance: 443 Infrastruktur-Hauptserver: 443
Globaler Katalog		Globaler Katalog: 3268, 3269

Mindestspeicherplatz

Abbildung 1-1. Mindestspeicherplatz für die kleine Konfiguration von vRealize Automation



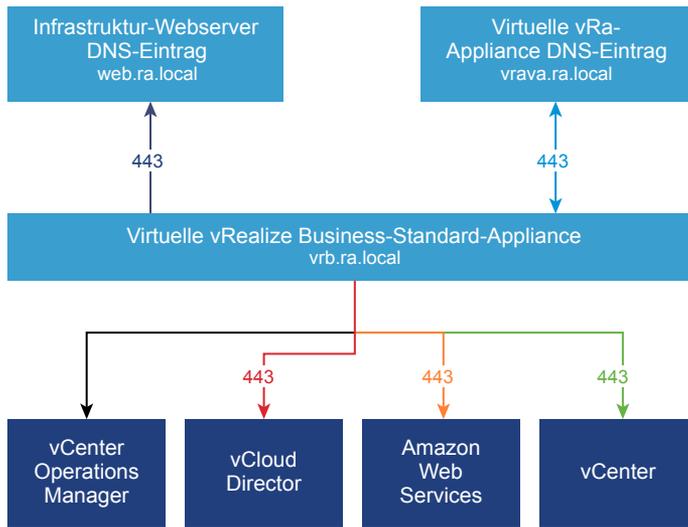
Nicht angezeigt:
Alle Infrastruktursysteme benötigen Zugriff auf Port 5480 aller vRealize-Appliances zur Protokollerfassung (vRA-Einstellungen > Cluster > Protokolle erfassen unter Virtual Appliance:5480), um zu funktionieren.

Für die VM-Remote-Konsole benötigt die vRealize-Appliance Zugriff auf VMware ESXi-Port 902 und der Infrastruktur- Hauptserver benötigt Zugriff auf Port 443 für den vSphere-Endpoint.

*Im Abschnitt „Datenbankbereitstellung“ finden Sie Informationen zum Eingrenzen dieses Bereichs.

Weiterhin ist eine bidirektionale Kommunikation erforderlich.

Abbildung 1-2. Mindestspeicherplatz für die kleine Konfiguration von vRealize Business for Cloud



Anforderungen an mittlere vRealize Automation -Bereitstellungen

Eine mittlere vRealize Automation-Bereitstellung umfasst Systeme mit 30.000 verwalteten Maschinen oder weniger mit den entsprechenden Maschinen, Lastausgleichsdiensten und Portkonfigurationen.

Support

Eine mittlere Bereitstellung kann die folgenden Elemente unterstützen.

- 30.000 verwaltete Maschinen
- 1000 Katalogelemente
- Bereitstellung von 50 Maschinen

Anforderungen

Eine mittlere Bereitstellung muss die entsprechenden Anforderungen an die Systemkonfiguration erfüllen.

Virtuelle Appliances

- vRealize Automation-Appliance 1: vrava-1.ra.local
- vRealize Automation-Appliance 2: vrava-2.ra.local
- vRealize Automation-Appliance 3: vrava-3.ra.local
- vRealize Business for Cloud-Appliance: vrb.ra.local

Virtuelle Windows Server-Maschinen

- Infrastruktur-Webserver/-Manager-Server 1 (Active Web oder DEM-O, Active Manager): inf-1.ra.local
- Infrastruktur-Webserver/-Manager-Server 2 (Active Web oder DEM-O, Passive Manager): inf-2.ra.local

- Infrastruktur-DEM-Server 1: dem-1.ra.local
- Infrastruktur-DEM-Server 2: dem-2.ra.local
- Infrastruktur-Agent-Server 1: agent-1.ra.local
- Infrastruktur-Agent-Server 2: agent-2.ra.local

Datenbankserver

- MSSQL-Failover-Cluster-Instanz: mssql.ra.local

Lastausgleichsdienste

- vRealize Automation-Appliance-Lastausgleichsdienst: med-vrava.ra.local
- Lastausgleichsdienst für Infrastruktur-Web: med-web.ra.local
- Lastausgleichsdienst für Infrastruktur-Manager Service: med-manager.ra.local

Zertifikate

Bei den in dieser Tabelle verwendeten Hostnamen handelt es sich nur um Beispiele.

Serverrolle	CN oder SAN
vRealize Automation-Appliance	SAN enthält die folgenden Hostnamen: <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local
Infrastruktur-Webserver oder -Manager-Server	SAN enthält die folgenden Hostnamen: <ul style="list-style-type: none"> ■ web.ra.local ■ manager.ra.local ■ inf-1.ra.local ■ inf-2.ra.local
vRealize Business for Cloud-Appliance	CN = vrb.ra.local

Ports

Benutzer benötigen Zugriff auf bestimmte Ports. Alle aufgelisteten Ports sind Standardports.

Serverrolle	Port
vRealize Automation-Appliance-Lastausgleichsdienst	443, 8444. Port 8444 ist für die VM-Remote-Konsole erforderlich.

Neben den für Benutzer erforderlichen Ports benötigen Administratoren Zugriff auf bestimmte Ports.

Serverrolle	Port
vRealize Automation-Appliance fVAMI	5480, 8443. Port 8443 ist für die erweiterte Konfiguration der Identitätsverwaltung reserviert. VMware Identity Manager zu Active Directory: 389, 636, 3268, 3269 VMware Identity Manager zu Domänen-Controller: 88, 464, 135
Control-Center des vRealize Appliance-Orchestrators	8283
vRealize Business for Cloud-Server	5480

Die folgende Tabelle zeigt die Kommunikation, die innerhalb der Anwendung stattfindet.

Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
vRealize Automation-Appliance	HTTPS: Adapterkonfiguration: 8443 Remote-Konsolenproxy: 8444 Postgres: 5432 RabbitMQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22	LDAP:389 LDAPS: 636 vRealize Automation-Appliance (alle anderen): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 vRealize Automation-Lastausgleichsdiens für Infrastruktur-Web: 443 VMware ESXi: 902. Infrastruktur-Webserver oder -Manager-Server benötigt Zugriff auf Port 443 für den vSphere-Endpoint, um ein Ticket für die VM-Remote-Konsole abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. Kerberos-Authentifizierung: 88 Computer-Objektkennwortverlängerung: 464
Infrastruktur-Webserver/-Manager-Server	HTTPS: 443 MSDTC: 135, 1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	vRealize Automation-Appliance-Lastausgleichsdiens: 443 vRealize Automation-Lastausgleichsdiens für Infrastruktur-Web: 443 vRealize Automation-Appliance (VA): 5480. vSphere-Endpoint: 443. Infrastruktur-Webserver oder -Manager-Server benötigt Zugriff auf Port 443 für den vSphere-Endpoint, um ein Ticket für die VM-Remote-Konsole abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. MSSQL: 135, 1433, 1024 to 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .
Infrastruktur-DEM-Server	–	Lastausgleichsdiens für vRealize Automation-Appliance: 443 vRealize Automation-Lastausgleichsdiens für Infrastruktur-Web: 443 vRealize Automation-Lastausgleichsdiens für Infrastruktur-Manager: 443 vRealize Automation-Appliance (VA): 5480.

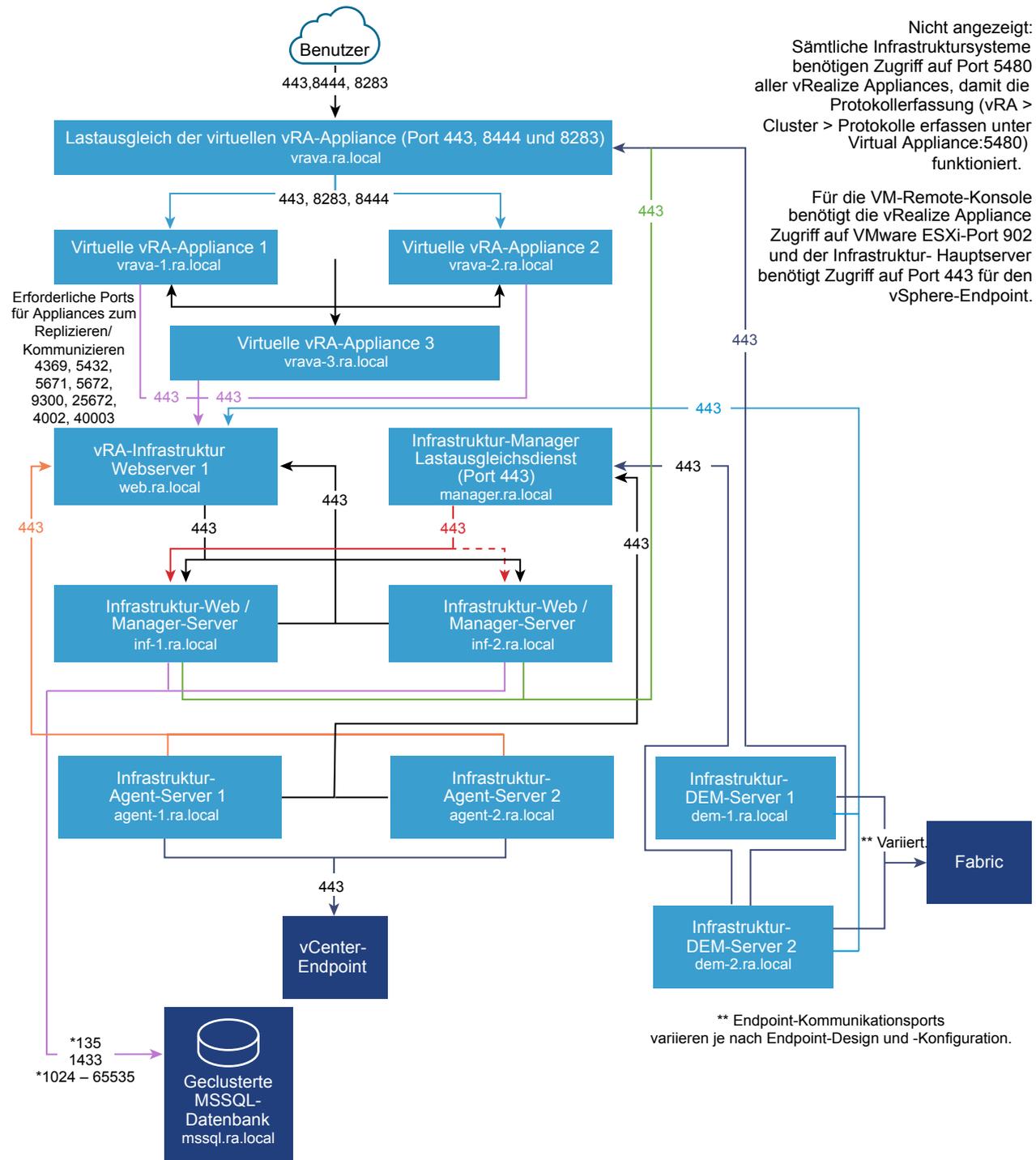
Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
Infrastruktur-Agent-Server	–	vRealize Automation-Lastausgleichs- dienst für Infrastruktur-Web: 443 vRealize Automation-Lastausgleichs- dienst für Infrastruktur-Manager: 443 vRealize Automation-Appliance (VA): 5480.
MSSQL-Datenbankserver	MSSQL: 1433 MSDTC: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbank- bereitstellung“ von vRealize Automation- Bereitstellung .	Infrastruktur-Webserver/-Manager-Ser- ver: 135, 1024 - 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstel- lung“ von vRealize Automation-Bereit- stellung .
vRealize Business for Cloud-Server	HTTPS: 443 SSH: 22 Verwaltungskonsole der virtuellen Appli- ance: 5480	Lastausgleichsdienst für vRealize Automation-Appliance: 443 vRealize Automation-Lastausgleichs- dienst für Infrastruktur-Web: 443
Globaler Katalog		Globaler Katalog: 3268, 3269

Lastausgleichsdienste benötigen Zugriff über die folgenden Ports.

Lastausgleichsdienst	Ausgeglichene Ports
vRealize Automation-Appliance-Lastausgleichsdienst	443, 8444
vRealize Automation-Lastausgleichsdienst für Infrastruktur- Web	443
Lastausgleichsdienst für vRealize Automation-Infrastruktur-Ma- nager Service	443

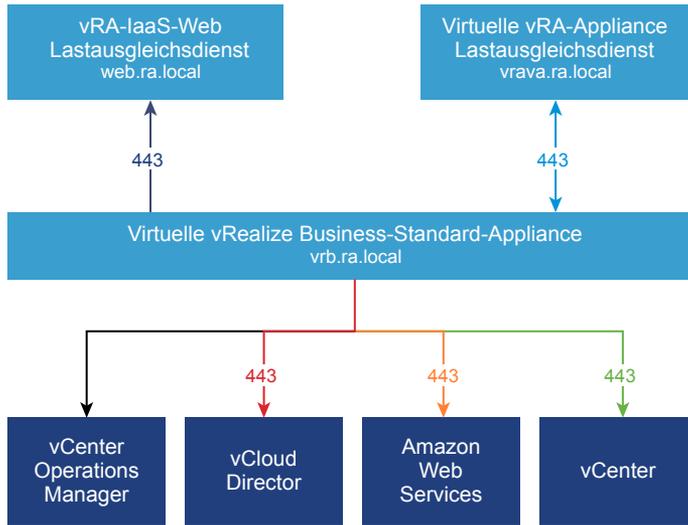
Grafik

Abbildung 1-3. Mindestspeicherplatz für die mittlere Konfiguration von vRealize Automation



*Im Abschnitt „Datenbankbereitstellung“ finden Sie Informationen zum Eingrenzen dieses Bereichs. Weiterhin ist eine bidirektionale Kommunikation erforderlich.

Abbildung 1-4. Mindestspeicherplatz für die mittlere Bereitstellung von vRealize Business for Cloud



Anforderungen an große vRealize Automation -Bereitstellungen

Eine große vRealize Automation-Bereitstellung umfasst Systeme mit 50.000 verwalteten Maschinen oder weniger mit den entsprechenden Maschinen, Lastausgleichsdiensten und Portkonfigurationen.

Support

Eine große Bereitstellung kann die folgenden Elemente unterstützen.

- 50.000 verwaltete Maschinen
- 2500 Katalogelemente
- Gleichzeitige Bereitstellung von 100 Maschinen

Anforderungen

Eine große Bereitstellung muss die entsprechenden Anforderungen an die Systemkonfiguration erfüllen.

Virtuelle Appliances

- vRealize Automation-Appliance 1: vrava-1.ra.local
- vRealize Automation-Appliance 2: vrava-2.ra.local
- vRealize Automation-Appliance 2: vrava-3.ra.local
- vRealize Automation-Appliance Appliance: vrb.ra.local

Virtuelle Windows Server-Maschinen

- Infrastruktur-Webserver 1: web-1.ra.local
- Infrastruktur-Webserver 2: web-2.ra.local

- Infrastruktur-Manager-Server 1: manager-1.ra.local
- Infrastruktur-Manager-Server 2: manager-2.ra.local
- Infrastruktur-DEM-Server 1: dem-1.ra.local
- Infrastruktur-DEM-Server 2: dem-2.ra.local
- Infrastruktur-Agent-Server 1: agent-1.ra.local
- Infrastruktur-Agent-Server 2: agent-2.ra.local
- Geclusterte MSSQL-Datenbank: mssql.ra.local

Lastausgleichsdienste

- Lastausgleichsdienst für vRealize Automation-Appliance: vrava.ra.local
- Lastausgleichsdienst für Infrastruktur-Web: web.ra.local
- Lastausgleichsdienst für Infrastruktur-Manager Service: manager.ra.local

Zertifikate

Bei den in dieser Tabelle verwendeten Hostnamen handelt es sich nur um Beispiele.

Serverrolle	CN oder SAN
vRealize Automation-Appliance	SAN enthält die folgenden Hostnamen: <ul style="list-style-type: none"> ▪ vrava.ra.local ▪ vrava-1.ra.local ▪ vrava-2.ra.local
Infrastruktur-Webserver	SAN enthält die folgenden Hostnamen: <ul style="list-style-type: none"> ▪ web.ra.local ▪ web-1.ra.local ▪ web-2.ra.local
Infrastruktur-Manager-Server	SAN enthält die folgenden Hostnamen: <ul style="list-style-type: none"> ▪ manager.ra.local ▪ manager-1.ra.local ▪ manager-2.ra.local
vRealize Business for Cloud-Appliance	CN = vrb.ra.local

Ports

Benutzer benötigen Zugriff auf bestimmte Ports. Alle aufgelisteten Ports sind Standardports.

Serverrolle	Port
Lastausgleichsdienst für vRealize Automation-Appliance	443, 8444 Port 88444 ist für die VMware Remote Console erforderlich.

Neben den für Benutzer erforderlichen Ports benötigen Administratoren Zugriff auf bestimmte Ports.

Serverrolle	Port
vRealize Automation-Appliance	5480, 8443. Port 8443 ist für die erweiterte Konfiguration der Identitätsverwaltung reserviert. VMware Identity Manager zu Active Directory: 389, 636, 3268, 3269 VMware Identity Manager zu Domänen-Controller: 88, 464, 135
vRealize Business for Cloud-Server	5480

Das System muss die entsprechenden Kommunikationen innerhalb der Anwendung unterstützen.

Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
vRealize Automation		
vRealize Automation-Appliance	HTTPS: 443 Adapterkonfiguration: 8443 Remote-Konsolenproxy: 8444 Postgres: 5432 Rabbit MQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 Control-Center: 8283	LDAP: 389 LDAPS: 636 vRealize Automation-Appliance: 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. vRealize Automation-Lastausgleichs-dienst für Infrastruktur-Web: 443 VMware ESXi: 902. Infrastruktur-Web benötigt Zugriff auf vSphere-Endpoint-Port 443, um ein Ticket für die VMware Remote Console abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. Kerberos-Authentifizierung: 88 Computer-Objektkennwortverlängerung: 464
Infrastruktur-Webserver	HTTPS: 443 MSDTC: 443, 1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	Lastausgleichs-dienst für vRealize Automation-Appliance: 443 Virtuelle Appliance für vRealize Automation-Appliance: 5480. vSphere-Endpoint: 443. Infrastruktur-Web benötigt Zugriff auf vSphere-Endpoint-Port 443, um ein Ticket für die VMware Remote Console abzurufen. Die vRealize Automation-Appliance benötigt Zugriff auf Port 902 für den ESXi-Host, um dem Benutzer Konsolendaten zu übermitteln. MSSQL: 135, 1433, 1024 to 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .

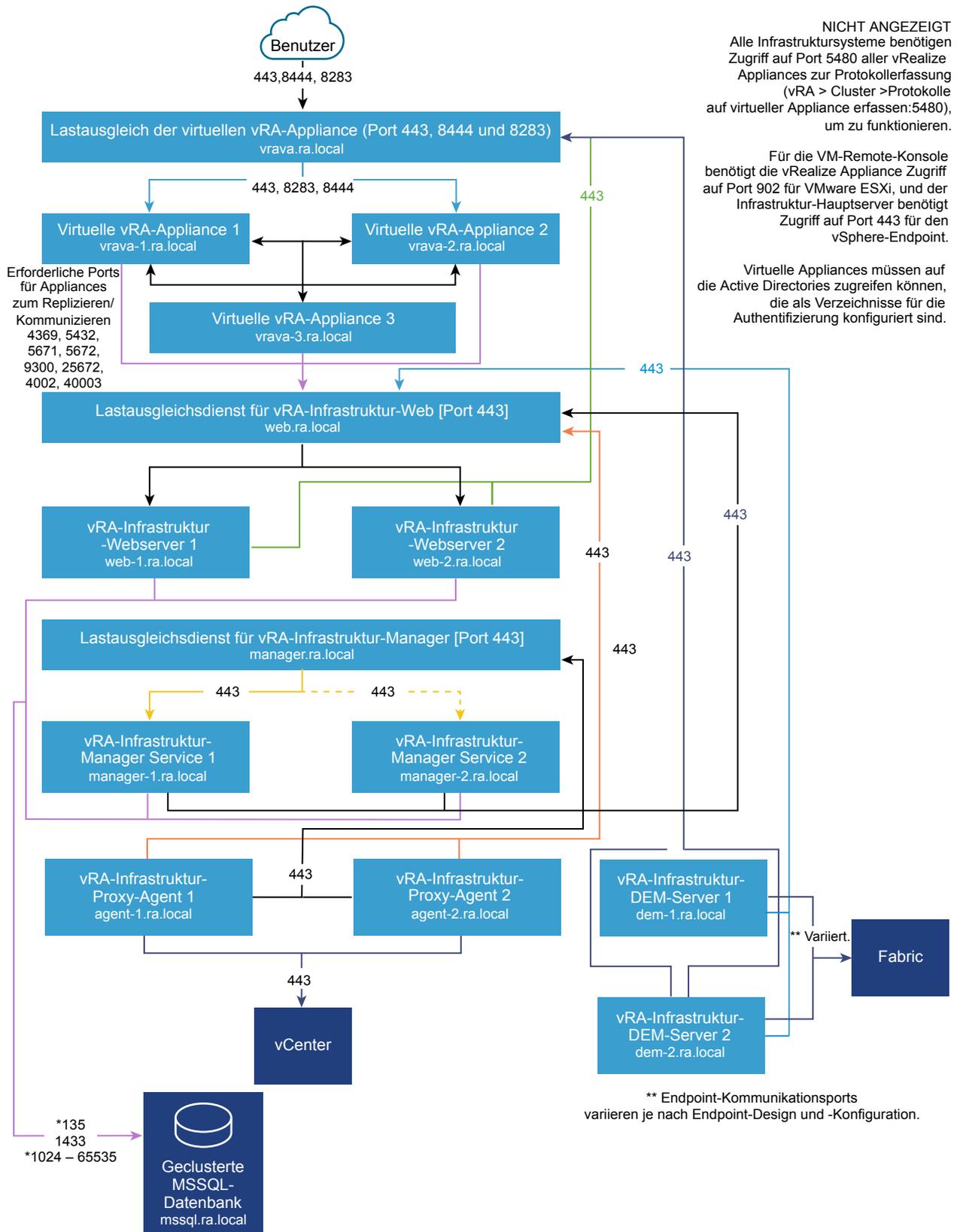
Serverrolle	Eingehende Ports	Ausgehende Ports für Service oder System
Infrastruktur-Manager-Server	HTTPS: 443 MSDTC: 135,1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	Lastausgleichsdienst für vRealize Automation-Appliance: 443 vRealize Automation-Lastausgleichsdienst für Infrastruktur-Web: 443 vRealize Automation-Appliance: 443, 5480 MSSQL: 135, 1433, 1024 to 65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .
Infrastruktur-DEM-Server	–	Lastausgleichsdienst für vRealize Automation-Appliance: 443 vRealize Automation-Lastausgleichsdienst für Infrastruktur-Web: 443 vRealize Automation-Lastausgleichsdienst für Infrastruktur-Manager: 443 vRealize Orchestrator-Lastausgleichsdienst: 8281 vRealize Automation-Appliance: 5480.
Infrastruktur-Agent-Server	–	vRealize Automation-Lastausgleichsdienst für Infrastruktur-Web: 443 vRealize Automation-Lastausgleichsdienst für Infrastruktur-Manager: 443 vRealize Automation-Appliance: 5480.
MSSQL-Datenbankserver	MSSQL: 1433 MSDTC: 135, 1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .	Infrastruktur-Webserver: 135, 1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung . Infrastruktur-Manager-Server: 135, 1024-65535. Informationen zur Eingrenzung dieses Bereichs finden Sie im Abschnitt „Datenbankbereitstellung“ von vRealize Automation-Bereitstellung .
vRealize Business for Cloud-Server	HTTPS: 443 SSH: 22 Verwaltungskonsole der virtuellen Appliance: 5480	Lastausgleichsdienst für vRealize Automation-Appliance: 443 vRealize Automation-Lastausgleichsdienst für Infrastruktur-Web: 443
Globaler Katalog		Globaler Katalog: 3268, 3269

Lastausgleichsdienste benötigen Zugriff über die folgenden Ports.

Lastausgleichsdienst	Ausgeglichene Ports
Lastausgleichsdienst für vRealize Automation-Appliance	443, 8444
vRealize Automation-Lastausgleichsdienst für Infrastruktur-Web	443
vRealize Automation-Lastausgleichsdienst für Manager-Server	443

Grafik

Abbildung 1-5. Mindestspeicherplatz für die große Konfiguration von vRealize Automation



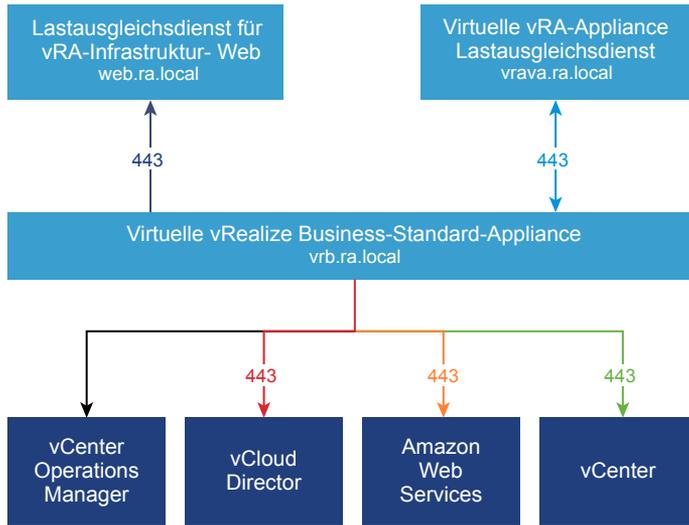
NICHT ANGEZEIGT
Alle Infrastruktursysteme benötigen Zugriff auf Port 5480 aller vRealize Appliances zur Protokollerfassung (vRA > Cluster > Protokolle auf virtueller Appliance erfassen:5480), um zu funktionieren.

Für die VM-Remote-Konsole benötigt die vRealize Appliance Zugriff auf Port 902 für VMware ESXi, und der Infrastruktur-Hauptserver benötigt Zugriff auf Port 443 für den vSphere-Endpoint.

Virtuelle Appliances müssen auf die Active Directories zugreifen können, die als Verzeichnisse für die Authentifizierung konfiguriert sind.

*Im Abschnitt „Datenbankbereitstellung“ finden Sie Informationen zum Eingrenzen dieses Bereichs. Weiterhin ist eine bidirektionale Kommunikation erforderlich.
VMware, Inc.

Abbildung 1-6. Mindestspeicherplatz für die große Konfiguration von vRealize Business for Cloud



Bereitstellung von Daten für mehrere vRealize Automation - Datencenter

vRealize Automation unterstützt die Verwaltung von Ressourcen in Remote-Datencentern.

Um vSphere-, HyperV- oder Xen-Ressourcen in Remote-Datencentern zu verwalten, stellen Sie den Proxy-Agent auf einer virtuellen Maschine im Remote-Datencenter bereit.

Hinweis Das folgende Diagramm zeigt eine vSphere-Bereitstellung. Andere Endpoints erfordern keine zusätzliche Konfiguration.

Da vRealize Orchestrator-Workflows möglicherweise über ein WAN kommunizieren, sollten Sie die im *Handbuch zum vRealize Orchestrator-Codierungsdesign* beschriebenen Best Practices befolgen.

Tabelle 1-3. Erforderliche Ports für die WAN-Kommunikation

Rolle	Eingehende Ports	Ausgehende Ports für Service oder System
vRealize Automation-Appliance – einschließlich eingebettetem vRealize Orchestrator	Nicht verfügbar	vSphere-Endpoint: 443 ESXi-Hosts: 903
vRealize Automation-Infrastruktur-Lastausgleichsdienst	vRealize Automation-Infrastruktur-Proxy-Agent: 443	Nicht verfügbar
vRealize Automation-Infrastruktur-Web-server	Nicht verfügbar	vSphere-Endpoint: 443

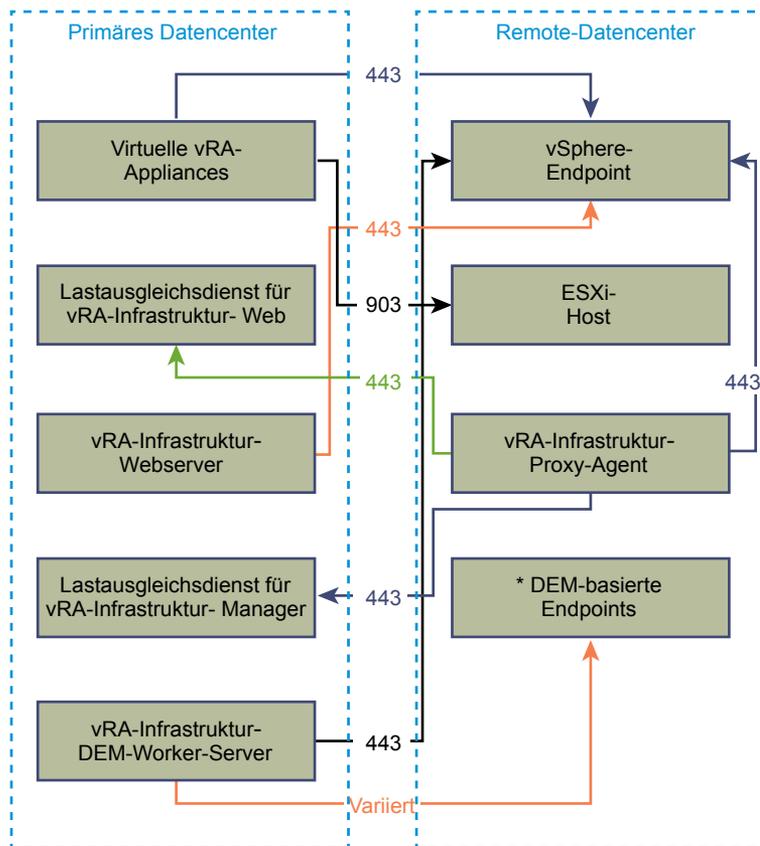
Tabelle 1-3. Erforderliche Ports für die WAN-Kommunikation (Fortsetzung)

Rolle	Eingehende Ports	Ausgehende Ports für Service oder System
Lastausgleichsdienst für vRealize Automation-Infrastruktur-Manager	vRealize Automation-Infrastruktur-Proxy-Agent: 443	Nicht verfügbar
vRealize Automation-Infrastruktur-DEM-Worker-Server	Nicht verfügbar	Endpoint: ** Variiert.

* Wenn DEM-Worker auf der Manager Service-Maschine oder einem anderen Server installiert sind, müssen diese Ports zwischen dieser Maschine und dem Ziel-Endpoint geöffnet sein.

** Der Port, der für die Kommunikation mit einem externen Endpoint erforderlich ist, variiert je nach Endpoint. Standardmäßig ist dies für vSphere Port 443.

Abbildung 1-7. vRealize Automation -Konfiguration mit mehreren Sites



Sichere Konfiguration von vRealize Automation

Sichere Konfiguration beschreibt, wie Sie das Sicherheitsprofil einer vRealize Automation-Bereitstellung gemäß den VMware-Richtlinien überprüfen, konfigurieren und aktualisieren.

Sichere Konfiguration umfasst die folgenden Themen:

- Sicherheit für die Softwareinfrastruktur
- Sicherheit für die bereitgestellte Konfiguration
- Sicherheit für das Hostnetzwerk

Sichere Baseline für vRealize Automation - Übersicht

VMware bietet umfassende Empfehlungen für das Überprüfen und Konfigurieren einer sicheren Baseline für Ihr vRealize Automation-System.

Verwenden Sie die von VMware angegebenen Tools und Verfahren, um eine gehärtete Baseline-Konfiguration für Ihr vRealize Automation-System zu erhalten. Einige vRealize Automation-Komponenten werden auf einer gehärteten bzw. teilweise gehärteten Basis installiert. Unter Berücksichtigung der VMware-Sicherheitsempfehlungen, Unternehmenssicherheitsrichtlinien und bekannten Bedrohungen sollten Sie jedoch alle Komponenten überprüfen und bestätigen.

vRealize Automation -Sicherheitsniveau

Das Sicherheitsniveau von vRealize Automation geht von einer ganzheitlich sicheren Umgebung basierend auf der System- und Netzwerkkonfiguration, den Sicherheitsrichtlinien des Unternehmens und den Best Practices zur Sicherheit aus.

Wenn Sie die Härtung eines vRealize Automation-Systems überprüfen und konfigurieren, beachten Sie die VMware-Empfehlungen zur Härtung in den folgenden Bereichen.

- Sichere Bereitstellung
- Sichere Konfiguration
- Netzwerksicherheit

Um sicherzustellen, dass Ihr System gehärtet ist, überprüfen Sie die VMware-Empfehlungen und Ihre lokalen Sicherheitsrichtlinien, da diese sich auf die genannten konzeptionellen Bereiche beziehen.

Systemkomponenten

Stellen Sie für die Härtung und sichere Konfiguration Ihres vRealize Automation-Systems sicher, dass Sie die Funktionsweise aller Komponenten und ihr Zusammenspiel hinsichtlich der Unterstützung der Systemfunktionalität kennen.

Beachten Sie bei der Planung und Implementierung eines sicheren Systems die folgenden Komponenten.

- vRealize Automation-Appliance
- IaaS-Komponente

Wenn Sie sich mit vRealize Automation und dem Zusammenspiel der Komponenten vertraut machen möchten, finden Sie hilfreiche Informationen unter [Grundlagen und Konzepte](#) im VMware vRealize Automation-Dokumentationscenter. Informationen zu den typischen Bereitstellungen und der Architektur von vRealize Automation finden Sie unter [vRealize Automation-Referenzarchitektur](#).

Überprüfen der Integrität der Installationsmedien

Benutzer sollten vor der Installation eines VMware-Produkts immer die Integrität der Installationsmedien überprüfen.

Überprüfen Sie nach dem Download eines ISO-Images, Offline-Pakets oder Patches stets den SHA1-Hashwert, um die Integrität und Authentizität der heruntergeladenen Dateien sicherzustellen. Wenn Sie physische Medien von VMware erhalten und das Sicherheitssiegel beschädigt ist, schicken Sie die Software an VMware zurück, um Ersatz zu erhalten.

Nach dem Herunterladen der Medien überprüfen Sie mithilfe des MD5/SHA1-Summenwerts die Integrität des Downloads. Vergleichen Sie die ausgegebene MD5/SHA1-Summe mit dem auf der VMware-Website angegebenen Wert. SHA1- oder MD5-Hashwert müssen übereinstimmen.

Weitere Informationen zum Überprüfen der Integrität der Installationsmedien finden Sie unter <http://kb.vmware.com/kb/1537>.

Härtung der Softwareinfrastruktur für VMware -Systeme

Bewerten Sie im Rahmen der Härtung die bereitgestellte Softwareinfrastruktur, die Ihr VMware-System unterstützt, und stellen Sie sicher, dass die Richtlinien zur Härtung von VMware eingehalten werden.

Überprüfen Sie vor der Härtung Ihres VMware-Systems die unterstützende Softwareinfrastruktur und beheben Sie mögliche Sicherheitsschwachstellen, um eine vollständig gehärtete Umgebung einzurichten. Bei den möglichen Softwareinfrastruktur-Elementen handelt es sich um Betriebssystemkomponenten, unterstützende Software und Datenbanksoftware. Räumen Sie Sicherheitsbedenken bei diesen und anderen Komponenten entsprechend den Empfehlungen des Herstellers und anderen relevanten Sicherheitsprotokollen aus.

Härtung der VMware vSphere[®] -Umgebung

Bewerten Sie die VMware vSphere[®]-Umgebung und stellen Sie sicher, dass ein angemessener Grad an vSphere-Härtung durchgesetzt und aufrecht erhalten wird.

Weitere Informationen zur Härtung finden Sie unter <http://www.vmware.com/security/hardening-guides.html>.

Im Rahmen einer umfassend gehärteten Umgebung muss die VMware vSphere[®]-Infrastruktur den in VMWaredefinierten Sicherheitsrichtlinien entsprechen.

Härtung des Infrastructure as a Service-Hosts

Stellen Sie sicher, dass Ihre Infrastructure as a Service-Hostmaschine unter Microsoft Windows gemäß der VMware-Richtlinien gehärtet ist.

Überprüfen Sie die Empfehlungen in den jeweiligen von Microsoft Windows empfohlenen Richtlinien zur Härtung und stellen Sie sicher, dass Ihr Windows Server-Host entsprechend gehärtet ist. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitschwachstellen über unsichere Komponenten von Windows-Versionen führen.

Informationen darüber, ob Ihre Version unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation Support](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung bei der Härtung von Microsoft-Produkten an.

Härtung von Microsoft SQL Server

Stellen Sie sicher, dass die Microsoft SQL Server-Datenbank die von Microsoft und VMware festgelegten Sicherheitsrichtlinien einhält.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von Microsoft SQL Server. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die installierte Version von Microsoft SQL Server. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitsschwachstellen über unsichere Komponenten von Microsoft SQL Server-Versionen führen.

Informationen darüber, ob Ihre Version von Microsoft SQL Server unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Härtung von Microsoft .NET

Im Rahmen einer umfassend gehärteten Umgebung muss Microsoft .NET die von Microsoft und VMware vorgeschriebenen Sicherheitsrichtlinien einhalten.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von .NET. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die von Ihnen verwendete Version von Microsoft SQL Server. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitsschwachstellen über unsichere Microsoft.NET-Komponenten führen.

Informationen darüber, ob Ihre Version von Microsoft.NET unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Härtung der Microsoft Internetinformationsdienste (IIS)

Stellen Sie sicher, dass Ihre Microsoft Internetinformationsdienste (IIS) alle von Microsoft und VMware vorgegebenen Sicherheitsrichtlinien einhalten.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von Microsoft IIS. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die von Ihnen verwendete Version von IIS. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann das zum Auftreten von bekannten Sicherheitsschwachstellen führen.

Informationen darüber, ob Ihre Version unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation Support](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Überprüfen der installierten Software

Da Schwachstellen in Software von Drittanbietern und nicht verwendeter Software das Risiko eines nicht autorisierten Systemzugriffs erhöhen und zu Unterbrechungen der Verfügbarkeit führen können, sollten Sie die gesamte auf den VMware-Hostmaschinen installierte Software überprüfen und ihre Verwendung bewerten.

Installieren Sie keine Software, die für den sicheren Betrieb des Systems auf den VMware-Hostmaschinen nicht erforderlich ist. Deinstallieren Sie nicht verwendete oder irrelevante Software.

In der Bestandsliste installierte nicht unterstützte Software

Bewerten Sie die VMware-Bereitstellung und den Bestand der installierten Produkte, um sicherzustellen, dass keine überflüssige nicht unterstützte Software installiert ist.

Weitere Informationen zu den Supportrichtlinien für Drittanbieterprodukte finden Sie im VMware Supportartikel unter <https://www.vmware.com/support/policies/thirdparty.html>.

Überprüfen von Drittanbietersoftware

VMware unterstützt oder empfiehlt nicht die Installation von Drittanbietersoftware, die nicht getestet und bestätigt wurde. Unsichere, nicht gepatchte oder nicht authentifizierte Drittanbietersoftware, die auf VMware-Hostmaschinen installiert ist, kann das System dem Risiko des unerlaubten Zugriffs aussetzen und zu Unterbrechungen der Verfügbarkeit führen. Wenn Sie nicht unterstützte Drittanbietersoftware verwenden müssen, wenden Sie sich an den Drittanbieter und informieren Sie sich über die Konfigurations- und Patching-Anforderungen.

Empfehlungen und Patches für die Sicherheit von VMware

Um die größtmögliche Sicherheit für Ihr System beizubehalten, beachten Sie die VMware-Sicherheitsempfehlungen und wenden Sie alle relevanten Patches an.

VMware hat Sicherheitsempfehlungen für Produkte veröffentlicht. Beachten Sie die Empfehlungen, um sicherzustellen, dass Ihr Produkt vor bekannten Bedrohungen geschützt ist.

Bewerten Sie die Installation, den Patch-Vorgang und den Upgrade-Verlauf von vRealize Automation und stellen Sie sicher, dass die veröffentlichten VMware-Sicherheitsempfehlungen befolgt und durchgesetzt werden.

Weitere Informationen zu den aktuellen VMware-Sicherheitsempfehlungen finden Sie unter <http://www.vmware.com/security/advisories/>.

Sichere Konfiguration

Überprüfen und aktualisieren Sie die Sicherheitseinstellungen für virtuelle vRealize Automation-Appliances und die Infrastructure as a Service-Komponente gemäß den Anforderungen Ihrer Systemkonfiguration. Überprüfen und aktualisieren Sie darüber hinaus weitere Komponenten oder Anwendungen.

Die sichere Konfiguration einer vRealize Automation-Installation umfasst die Konfiguration jeder einzelnen Komponente, da alle Komponenten ein funktionierendes Ganzes bilden. Konfigurieren Sie alle Systemkomponenten in Abstimmung zueinander, um eine angemessen sichere Baseline zu erreichen.

Sichern der vRealize Automation -Appliance

Überprüfen und aktualisieren Sie die Sicherheitseinstellungen für die vRealize Automation-Appliance wie für die Systemkonfiguration erforderlich.

Konfigurieren Sie die Sicherheitseinstellungen für Ihre virtuellen Appliances und deren Hostbetriebssysteme. Legen Sie darüber hinaus die Konfiguration anderer zugehöriger Komponenten und Anwendungen fest oder überprüfen Sie sie. In einigen Fällen müssen Sie vorhandene Einstellungen überprüfen, während Sie für andere Einstellungen ändern oder hinzufügen müssen, um eine entsprechende Konfiguration zu erreichen.

Ändern des Root-Kennworts

Sie können das Root-Kennwort für die vRealize Automation-Appliance ändern, um die entsprechenden Sicherheitsanforderungen zu erfüllen.

Ändern Sie das Root-Kennwort in der vRealize Automation-Appliance unter Verwendung der Schnittstelle für die Verwaltung der virtuellen Appliance. Stellen Sie sicher, dass das Root-Kennwort die Komplexitätsanforderungen an Kennwörter in Ihrem Unternehmen erfüllt.

Verfahren

- 1 Öffnen Sie die Verwaltungsschnittstelle der virtuellen Appliance für Ihre vRealize Automation-Appliance.
`https://vRealizeAppliance-ur1:5480`
- 2 Wählen Sie die Registerkarte **Admin** auf der Verwaltungsschnittstelle der virtuellen Appliance aus.
- 3 Wählen Sie das **Admin**-Untermenü aus.
- 4 Geben Sie das vorhandene Kennwort in das Textfeld **Aktuelles Administratorkennwort** ein.
- 5 Geben Sie das neue Kennwort in das Textfeld **Neues Administratorkennwort** ein.
- 6 Geben Sie das neue Kennwort in das Textfeld **Neues Administratorkennwort erneut eingeben** ein.
- 7 Klicken Sie auf **Einstellungen speichern**, um Ihre Änderungen zu speichern.

Überprüfen des Root-Kennworthash und der Komplexität

Stellen Sie sicher, dass das Root-Kennwort die Komplexitätsanforderungen an Kennwörter in Ihrem Unternehmen erfüllt.

Das Überprüfen der Komplexität des Root-Kennworts ist erforderlich, da der Root-Benutzer die Komplexitätsprüfung des Kennworts mithilfe des pam_crackli-Moduls umgeht, das an Benutzerkonten angehängt ist.

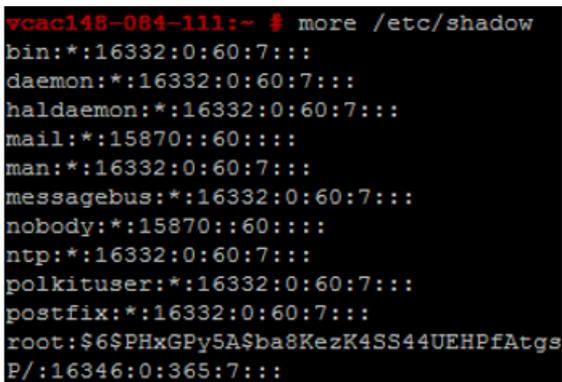
Das Kennwort des Kontos muss mit \$6\$ beginnen, was einen sha512-Hashwert anzeigt. Dies ist der standardmäßige Hashwert für alle gehärteten Appliances.

Verfahren

- 1 Um den Hashwert des Root-Kennworts zu überprüfen, melden Sie sich als Root-Benutzer an und führen den Befehl `# more /etc/shadow` aus.

Die Hashinformationen werden angezeigt.

Abbildung 1-8. Ergebnisse des Kennworthashes



```
vcac148-084-111:~ $ more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPy5A$ba8KezK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Wenn das Root-Kennwort keinen sha512-Hash enthält, führen Sie den `passwd`-Befehl aus, um ihn zu ändern.

Alle gehärteten Appliances verwenden `enforce_for_root` für das `pw_history`-Modul aus der Datei `etc/pam.d/common-password`. Standardmäßig speichert das System die letzten fünf Kennwörter. Alte Kennwörter werden für jeden Benutzer in der Datei `/etc/security/passwd` gespeichert.

Überprüfen des Root-Kennwortverlaufs

Stellen Sie sicher, dass der Kennwortverlauf für das Root-Konto durchgesetzt wird.

Alle gehärteten Appliances verwenden `enforce_for_root` für das `pw_history`-Modul aus der Datei `etc/pam.d/common-password`. Standardmäßig speichert das System die letzten fünf Kennwörter. Alte Kennwörter werden für jeden Benutzer in der Datei `/etc/security/passwd` gespeichert.

Verfahren

- 1 Führen Sie den folgenden Befehl aus:


```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```
- 2 Stellen Sie sicher, dass `enforce_for_root` in den zurückgegebenen Ergebnissen angezeigt wird.


```
passwd required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Verwalten des Kennwortablaufs

Konfigurieren Sie den Ablauf der Kennwörter aller Konten gemäß den Sicherheitsrichtlinien Ihres Unternehmens.

Standardmäßig verwenden alle Konten von gehärteten virtuellen VMware-Appliances einen Kennwortablauf von 60 Tagen. Auf den meisten gehärteten Appliances ist für das Root-Konto ein Kennwortablauf von 365 Tagen festgelegt. Überprüfen Sie im Sinne der Best Practice, dass die Ablaufzeit für alle Kontokennwörter sowohl die Sicherheits- als auch die Betriebsanforderungen erfüllt.

Wenn das Root-Kennwort abläuft, können Sie es nicht reaktivieren. Sie müssen standortspezifische Richtlinien hinzufügen, um zu verhindern, dass Administrator- und Root-Kennwörter ablaufen.

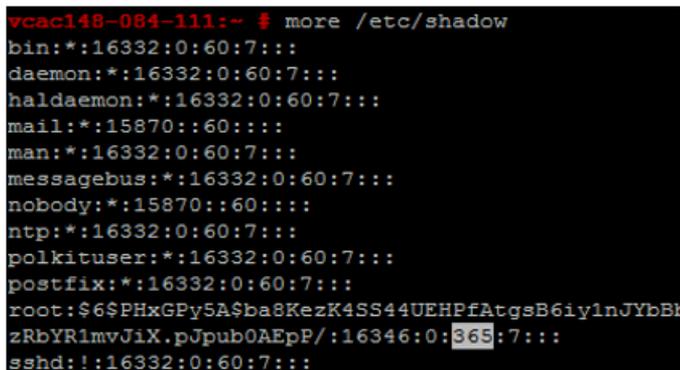
Verfahren

- 1 Melden Sie sich bei Ihren Maschinen mit virtuellen Appliances als Root-Benutzer an und führen Sie den folgenden Befehl aus, um den Kennwortablauf für alle Konten zu überprüfen.

```
# cat /etc/shadow
```

Der Kennwortablauf ist das fünfte Feld (Felder werden durch Doppelpunkte getrennt) der Shadow-Datei. Die Root-Ablaufdauer wird in Tagen festgelegt.

Abbildung 1-9. Feld „Kennwortablauf“



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KezK4SS44UEHPfAtgsB6iy1nJYbBkzRbYR1mvJiX.pJpub0AEP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Um den Ablauf des Root-Kontos zu ändern, führen Sie einen Befehl im folgenden Format aus.

```
# passwd -x 365 root
```

In diesem Befehl gibt 365 die Anzahl der Tage bis zum Ablauf des Kennworts an. Verwenden Sie denselben Befehl, um beliebige Benutzer zu ändern. Ersetzen Sie dabei das spezifische Konto für 'root' und die Anzahl der Tage, sodass sie die Standards für den Kennwortablauf der Organisation erfüllen.

Verwalten von Secure Shell und Administratorkonten

Für Remoteverbindungen umfassen alle gehärteten Appliances das Secure Shell (SSH)-Protokoll. Verwenden Sie SSH nur bei Bedarf und verwalten Sie diese Befehlszeilenumgebung zur Erhaltung der Systemsicherheit.

SSH ist eine interaktive Befehlszeilenumgebung, die Remoteverbindungen zu virtuellen VMware-Appliances unterstützt. Standardmäßig erfordert der SSH-Zugriff die Anmeldedaten eines Benutzerkontos mit weitreichenden Berechtigungen. Bei SSH-Aktivitäten von Root-Benutzern werden die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) und Überwachungssteuerung der virtuellen Appliance in der Regel umgangen.

Es wird empfohlen, SSH in einer Produktionsumgebung zu deaktivieren und nur dann zu aktivieren, wenn Probleme behoben werden müssen, die mit anderen Mitteln nicht behoben werden können. Lassen Sie SSH nur solange aktiviert, wie es für einen bestimmten Zweck erforderlich ist und wie es die Sicherheitsrichtlinien Ihres Unternehmens zulassen. SSH ist auf der vRealize Automation-Appliance standardmäßig deaktiviert. Je nach Ihrer vSphere-Konfiguration können Sie SSH aktivieren oder deaktivieren, wenn Sie Ihre OVF (Open Virtualization Format)-Vorlage bereitstellen.

Ein einfacher Test, um zu ermitteln, ob SSH auf einer Maschine aktiviert ist, besteht darin, zu versuchen, eine Verbindung unter Verwendung von SSH zu öffnen. Wenn die Verbindung geöffnet wird und Anmeldedaten abgefragt werden, ist SSH aktiviert und für Verbindungen verfügbar.

Secure Shell-Root-Benutzerkonto

Da VMware-Appliances keine vorkonfigurierten Benutzerkonten enthalten, kann SSH vom Root-Konto standardmäßig für eine direkte Anmeldung verwendet werden. Deaktivieren Sie SSH so schnell wie möglich als Boot-Benutzer.

Um die Übereinstimmungsstandards für Unleugbarkeit zu erfüllen, ist der SSH-Server auf allen gehärteten Appliances mit einem AllowGroups-Wheel-Eintrag vorkonfiguriert, um den SSH-Zugriff auf den sekundären Gruppen-Wheel-Eintrag einzuschränken. Um die Verantwortlichkeiten zu trennen, können Sie den AllowGroups-Wheel-Eintrag in der Datei `/etc/ssh/sshd_config` zwecks Verwendung einer anderen Gruppe, wie `sshd`, ändern.

Die Wheel-Gruppe ist mit dem `pam_wheel`-Modul für den Superuser-Zugriff aktiviert, sodass Mitglieder der Wheel-Gruppe `su-root` ausführen können, wenn das Root-Kennwort erforderlich ist. Eine Gruppentrennung ermöglicht Benutzern die Verwendung von SSH auf der Appliance, nicht aber die Ausführung von `su` auf `root`. Entfernen oder ändern Sie keine anderen Einträge im AllowGroups-Feld, um die ordnungsgemäße Funktionalität der Appliance sicherzustellen. Nach einer Änderung müssen Sie den SSH-Daemon neu starten, indem Sie diesen Befehl ausführen: `# service sshd restart`.

Aktivieren oder Deaktivieren von Secure Shell auf den vRealize Automation -Appliances

Aktivieren Sie Secure Shell (SSH) auf der vRealize Automation-Appliance nur zur Fehlerbehebung. Deaktivieren Sie SSH auf diesen Komponenten während des normalen Produktionsbetriebs.

Sie können SSH auf der vRealize Automation-Appliance mithilfe der Virtual Appliance Management-Konsole aktivieren oder deaktivieren.

Verfahren

- 1 Navigieren Sie zur Virtual Appliance Management-Konsole (VAMI) für Ihre vRealize Automation-Appliance.

: `https://vRealizeAppliance url:5480`

- 2 Klicken Sie auf die Registerkarte **Administrator**.
- 3 Klicken Sie auf das Untermenü **Administrator**.
- 4 Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **SSH-Dienst zu aktivieren**, um SSH zu aktivieren bzw. zu deaktivieren.
- 5 Klicken Sie auf **Einstellungen speichern**, um Ihre Änderungen zu speichern.

Erstellen eines lokalen Administratorkontos für Secure Shell

Erstellen und konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit lokale Administratorkonten für Secure Shell (SSH) auf den Hostmaschinen für virtuelle Appliances. Entfernen Sie auch den Root-SSH-Zugriff nach dem Erstellen der entsprechenden Konten.

Erstellen Sie lokale Administratorkonten für SSH oder Mitglieder der sekundären Wheel-Gruppe bzw. beides. Testen Sie vor dem Deaktivieren des direkten Root-Zugriffs, dass autorisierte Administratoren mit AllowGroups auf SSH zugreifen und mit der Wheel-Gruppe su auf root ausführen können.

Verfahren

- 1 Melden Sie sich bei der virtuellen Appliance als Root-Benutzer an und führen Sie die folgenden Befehle mit dem entsprechenden Benutzernamen aus.

```
# useradd -g users <username> -G wheel -m -d /home/benutzername  
# passwd username
```

Wheel ist die in AllowGroups angegebene Gruppe für den SSH-Zugriff. Um mehrere sekundäre Gruppen hinzuzufügen, verwenden Sie `-G wheel,sshd`.

- 2 Wechseln Sie zum Benutzer und geben Sie ein neues Kennwort ein, um die Prüfung der Kennwortkomplexität zu erzwingen.

```
# su -benutzername # benutzername@hostname  
# :~>passwd
```

Wenn die Kennwortkomplexität erfüllt wird, wird das Kennwort aktualisiert. Wenn die Kennwortkomplexität nicht erfüllt wird, wird das Kennwort auf das ursprüngliche Kennwort zurückgesetzt, und Sie müssen den Kennwortbefehl erneut ausführen.

- 3 Um die direkte Anmeldung bei SSH zu entfernen, ändern Sie die Datei `/etc/ssh/sshd_config` durch Ersetzen von `(#)PermitRootLogin yes` durch `PermitRootLogin no`.

Alternativ dazu können Sie in der Virtual Appliance Management Interface (VAMI) SSH aktivieren/deaktivieren, indem Sie das Kontrollkästchen **Administrator-SSH-Anmeldung aktiviert** auf der Registerkarte **Admin** aktivieren bzw. deaktivieren.

Nächste Schritte

Deaktivieren Sie direkte Anmeldungen als Root-Benutzer. Standardmäßig erlauben die gehärteten Appliances die direkte Anmeldung als Root-Benutzer über die Konsole. Nachdem Sie Administratorkonten für die Unleugbarkeit erstellt und diese für den Su-Root-Wheel-Zugriff getestet haben, deaktivieren Sie direkte Root-Anmeldungen durch Bearbeiten der Datei `/etc/security` als Root-Benutzer und Ersetzen des `tty1`-Eintrags durch `console`.

- 1 Öffnen Sie die Datei `/etc/securetty` in einem Texteditor.
- 2 Suchen Sie `tty1` und ersetzen Sie es durch `console`.
- 3 Speichern Sie die Datei und schließen Sie sie.

Härten der Secure Shell-Serverkonfiguration

Sofern möglich, weisen alle VMware-Appliances eine standardmäßige gehärtete Konfiguration auf. Benutzer können die ausreichende Härtung ihrer Konfiguration überprüfen, indem Sie die Server- und Client-Einstellungen im Abschnitt mit globalen Optionen der Konfigurationsdatei untersuchen.

Verfahren

- 1 Öffnen Sie die Konfigurationsdatei `/etc/ssh/sshd_config` auf der VMware-Appliance und stellen Sie sicher, dass die Einstellungen korrekt sind.

Einstellung	Status
Server-Daemon-Protokoll	Protokoll 2
CBC-Verschlüsselungen	aes256-ctr und aes128-ctr
TCP-Weiterleitung	AllowTCPForwarding Nein
Server-Gateway-Ports	Gateway-Ports Nein
X11-Weiterleitung	X11Forwarding, Nein
SSH-Dienst	Verwenden Sie das Feld „AllowGroups“ und geben Sie den zulässigen Zugriff für eine Gruppe an. Fügen Sie dieser Gruppe die passenden Mitglieder hinzu.
GSSAPI-Authentifizierung	GSSAPIAuthentication Nein, sofern nicht verwendet
Keberos-Authentifizierung	KeberosAuthentication Nein, sofern nicht verwendet
Lokale Variablen (globale AcceptEnv-Option)	Auf deaktiviert durch Auskommentieren oder für <code>LC_*</code> oder <code>LANG</code> -Variablen aktiviert festlegen
Tunnel-Konfiguration	PermitTunnel Nein
Netzwerksitzungen	MaxSessions 1
Gleichzeitige Benutzerverbindungen	Für Root- und andere Benutzer auf 1 festlegen. Die Datei <code>/etc/security/limits.conf</code> muss auch mit derselben Einstellung konfiguriert werden.
Überprüfung des strengen Modus	Strenge Modi Ja
Berechtigungstrennung	UsePrivilegeSeparation Ja
Rhosts RSA-Authentifizierung	RhostsESAAuthentication Nein

Einstellung	Status
Komprimierung	Komprimierung verzögert oder Komprimierung Nein
Meldungsauthentifizierungscode	MACs hmac-sha1
Benutzerzugriffseinschränkung	PermitUserEnvironment Nein

2 Speichern Sie die Änderungen und schließen Sie die Datei.

Härten der Secure Shell-Clientkonfiguration

Bewerten Sie im Rahmen der Härtung Ihres Systems die Härtung des SSH-Clients, indem Sie die SSH-Clientkonfigurationsdatei auf den Hostmaschinen der virtuellen Appliance überprüfen und sicherstellen, dass die VMware-Richtlinien eingehalten werden.

Verfahren

1 Öffnen Sie die SSH-Clientkonfigurationsdatei `/etc/ssh/ssh_config` und stellen Sie sicher, dass die Einstellungen im Abschnitt mit den globalen Optionen korrekt sind.

Einstellung	Status
Clientprotokoll	Protokoll 2
Client-Gateway-Ports	Gateway-Ports Nein
GSSAPI-Authentifizierung	GSSAPIAuthentication Nein
Lokale Variablen (globale <code>SendEnv-Option</code>)	Nur <code>LC_*</code> oder LANG-Variablen angeben
CBC-Verschlüsselungen	nur <code>aes256-ctr</code> und <code>aes128-ctr</code>
Meldungsauthentifizierungscode	Nur im MACs <code>hmac-sha1</code> -Eintrag verwendet

2 Speichern Sie die Änderungen und schließen Sie die Datei.

Überprüfen von Berechtigungen für Secure Shell-Schlüsseldateien

Um die Wahrscheinlichkeit von Angriffen zu minimieren, behalten Sie kritische Berechtigungen für SSH-Schlüsseldateien auf den Hostmaschinen Ihrer virtuellen Appliances bei.

Stellen Sie nach dem Konfigurieren oder Aktualisieren Ihrer SSH-Konfiguration immer sicher, dass die folgenden Berechtigungen für SSH-Schlüsseldateien nicht geändert werden.

- Die Schlüsseldateien für öffentliche Hosts in `/etc/ssh/*key.pub` gehören dem Root-Benutzer, und die Berechtigungen für diese Dateien sind auf `0644 (-rw-r--r-)` festgelegt.
- Die Schlüsseldateien für private Hosts in `/etc/ssh/*key` gehören dem Root-Benutzer, und die Berechtigungen für diese Dateien sind auf `0600 (-rw-----)` festgelegt.

Überprüfen der SSH-Berechtigungen für Schlüsseldateien

Stellen Sie sicher, dass SSH-Berechtigungen auf öffentliche und private Schlüsseldateien angewendet werden.

Verfahren

- 1 Überprüfen Sie die öffentlichen SSH-Schlüsseldateien, indem Sie folgenden Befehl ausführen: `ls -l /etc/ssh/*key.pub`
- 2 Stellen Sie sicher, dass als Besitzer und Gruppenbesitzer Root festgelegt ist und dass die Berechtigungen für die Dateien auf 0644 (-rw-r--r-) festgelegt wurden.
- 3 Lösen Sie etwaige Probleme, indem Sie die folgenden Befehle ausführen.

```
chown root /etc/ssh/*key.pub  
chgrp root /etc/ssh/*key.pub  
chmod 644 /etc/ssh/*key.pub
```
- 4 Überprüfen Sie die privaten SSH-Schlüsseldateien, indem Sie folgenden Befehl ausführen: `ls -l /etc/ssh/*key`
- 5 Lösen Sie etwaige Probleme, indem Sie die folgenden Befehle ausführen.

```
chown root /etc/ssh/*key  
chgrp root /etc/ssh/*key  
chmod 644 /etc/ssh/*key
```

Ändern des Benutzers der Verwaltungsschnittstelle für die virtuelle Appliance

Sie können Benutzer in der Verwaltungsschnittstelle der virtuellen Appliance hinzufügen und löschen, um für das gewünschte Maß an Sicherheit zu sorgen.

Das Root-Benutzerkonto für die Verwaltungsschnittstelle der virtuellen Appliance verwendet PAM für die Authentifizierung. Daher finden hier die Clipping-Ebenen von PAM Anwendung. Wenn Sie die Verwaltungsschnittstelle der virtuellen Appliance nicht ordnungsgemäß isoliert haben, kann das Root-Konto blockiert werden, wenn ein Angreifer versucht, eine Anmeldung zu erzwingen. Darüber hinaus können Sie den Admin-Benutzer für die Verwaltungsschnittstelle ändern, wenn mehrere Personen in Ihrer Organisation das Root-Konto für die Unleugbarkeit nicht für ausreichend halten.

Voraussetzungen

Verfahren

- 1 Führen Sie den folgenden Befehl aus, um einen neuen Benutzer zu erstellen und ihn zu der Verwaltungsschnittstellengruppe der virtuellen Appliance hinzuzufügen.

```
useradd -G vami,root Benutzer
```
- 2 Erstellen Sie ein Kennwort für den Benutzer.

```
passwd Benutzer
```

- 3 (Optional) Führen Sie den folgenden Befehl aus, um den Root-Zugriff auf die Verwaltungsschnittstelle der virtuellen Appliance zu deaktivieren.

```
usermod -R vami root
```

Hinweis Durch das Deaktivieren des Root-Zugriffs auf die Verwaltungsschnittstelle der virtuellen Appliance wird auch die Möglichkeit deaktiviert, den Administrator, den Root-Administrator oder das Kennwort über die Registerkarte Admin zu ändern.

Festlegen der Bootloader-Authentifizierung

Um einen angemessenen Grad an Sicherheit bereitzustellen, konfigurieren Sie Bootloader-Authentifizierung auf Ihren virtuellen VMware-Appliances.

Wenn der Bootloader des Systems keine Authentifizierung erfordert, können Benutzer mit Zugriff auf die Systemkonsole die Konfiguration für das Starten des Systems ändern oder das System im Einzelbenutzer- oder Wartungsmodus starten, was zu einem Denial-of-Service oder zu nicht autorisiertem Zugriff führen kann. Da die Bootloader-Authentifizierung auf virtuellen VMware-Appliances nicht standardmäßig festgelegt ist, müssen Sie ein GRUB-Kennwort erstellen, um sie zu konfigurieren.

Verfahren

- 1 Überprüfen Sie, ob ein Boot-Kennwort vorhanden ist, indem Sie die `password --md5 <password-hash>`-Zeile der Datei `/boot/grub/menu.lst` auf Ihrer virtuellen Appliance suchen.
- 2 Wenn kein Kennwort vorhanden ist, führen Sie den `# /usr/sbin/grub-md5-crypt`-Befehl für Ihre virtuelle Appliance aus.

Ein MD5-Kennwort wird generiert, und der Befehl liefert die md5-Hash-Ausgabe.
- 3 Fügen Sie das Kennwort der Datei `menu.lst` an, indem Sie den `# password --md5 <hash from grub-md5-crypt>`-Befehl ausführen.

Konfigurieren von NTP

Für die kritische Zeitermittlung deaktivieren Sie die Hostzeitsynchronisierung und verwenden Sie das Network Time Protocol (NTP) auf der vRealize Automation-Appliance.

Der NTP-Daemon auf der vRealize Automation-Appliance stellt synchronisierte Zeitdienste bereit. NTP ist standardmäßig deaktiviert, daher müssen Sie es manuell konfigurieren. Verwenden Sie möglichst NTP in Produktionsumgebungen, um Benutzeraktionen zu verfolgen und potenziell schädliche Angriffe und böswillige Eindringversuche durch akkurate Überwachung und Protokollführung zu erkennen. Informationen zu NTP-Sicherheitshinweisen finden Sie auf der NTP-Website.

Die NTP-Konfigurationsdatei befindet sich im Ordner `/etc/` auf jeder Appliance. Sie können den NTP-Dienst für die vRealize Automation-Appliance aktivieren und Zeitserver auf der Registerkarte **Admin** der Verwaltungsschnittstelle der virtuellen Appliance hinzufügen.

Verfahren

- 1 Öffnen Sie die Konfigurationsdatei `/etc/ntp.conf` auf der Hostmaschine der virtuellen Appliance in einem Texteditor.

- 2 Setzen Sie den Dateibesitzer auf **root:root**.
- 3 Setzen Sie die Berechtigungen auf **0640**.
- 4 Um das Risiko für einen Denial-of-Service-Verstärkungsangriff auf den NTP-Dienst zu verringern, öffnen Sie die Datei `/etc/ntp.conf` und vergewissern Sie sich, dass die eingeschränkten Zeilen in der Datei angezeigt werden.

```
restrict default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery  
restrict 127.0.0.1  
restrict -6 ::1
```

- 5 Speichern Sie die Änderungen und schließen Sie die Dateien.

Konfigurieren von TLS für übertragene Daten der vRealize Automation -Appliance

Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung starke TLS-Protokolle verwendet, um Übertragungskanäle für Komponenten der vRealize Automation-Appliance zu sichern.

Aus Leistungsgründen ist TLS für Localhost-Verbindungen zwischen einigen Anwendungsdiensten nicht aktiviert. In Fällen, bei denen ein umfassender Schutz von Bedeutung ist, aktivieren Sie TLS für alle localhost-Kommunikationen.

Wichtig Wenn Sie TLS auf dem Lastausgleichsdienst beenden, deaktivieren Sie unsichere Protokolle wie SSLv2, SSLv3 und TLS 1.0 auf allen Lastausgleichsdiensten.

Aktivieren von TLS für die Localhost-Konfiguration

Für einige Localhost-Kommunikationen wird TLS standardmäßig nicht verwendet. Sie können TLS über alle Localhost-Verbindungen zum Erhöhung der Sicherheit aktivieren.

Verfahren

- 1 Stellen Sie eine Verbindung mit vRealize Automation-Appliance mithilfe von SSH her.
- 2 Legen Sie Berechtigungen für den `vcac-Keystore` fest, indem Sie die folgenden Befehle ausführen.

```
usermod -A vco,coredump,pivotal vco  
chown vcac.pivotal /etc/vcac/vcac.keystore  
chmod 640 /etc/vcac/vcac.keystore
```

3 Aktualisieren Sie die HAProxy-Konfiguration.

a Öffnen Sie die HAProxy-Konfigurationsdatei unter `/etc/haproxy/conf.d` und wählen Sie den Dienst `20-vcac.cfg` aus.

b Suchen Sie die Zeilen mit der folgenden Zeichenfolge:

```
server local 127.0.0.1... und fügen Sie Folgendes zum Ende von solchen Zeilen hinzu: ssl
verify none
```

Dieser Abschnitt enthält andere Zeilen ähnlich der folgenden:

backend-horizon	backend-vro
backend-vra	backend-artifactory
backend-vra-health	

c Ändern Sie den Port für „backend-horizon“ von 8080 in 8443.

4 Rufen Sie das Kennwort von keystorePass ab.

a Suchen Sie die Eigenschaft `certificate.store.password` in der Datei `/etc/vcac/security.properties`.

Beispielsweise `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

b Entschlüsseln Sie den Wert mit dem folgenden Befehl:

```
vcac-config prop-util -d --p VALUE
```

Beispielsweise `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 Konfigurieren Sie den Dienst vRealize Automation.

a Öffnen Sie die Datei `/etc/vcac/server.xml`.

b Fügen Sie das folgende Attribut des Konnektor-Tags hinzu und ersetzen Sie „`certificate.store.password`“ durch den Wert für das Zertifikatspeicherkenwort in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6 Konfigurieren Sie den vRealize Orchestrator-Dienst.

a Öffnen Sie die Datei `/etc/vco/app-server.xml`

b Fügen Sie das folgende Attribut des Konnektor-Tags hinzu und ersetzen Sie „`certificate.store.password`“ durch den Wert für das Zertifikatspeicherkenwort in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

- 7 Starten Sie die Dienste vRealize Orchestrator, vRealize Automation und haproxy neu.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Hinweis Wenn der vco-server nicht neu gestartet wird, starten Sie den Host-Computer neu.

- 8 Konfigurieren Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI).
 - a Öffnen Sie die Datei `/opt/vmware/share/htdocs/service/café-services/services.py`.
 - b Ändern Sie die Zeile `conn = httpLib.HTTP()` in `conn = httpLib.HTTPS()` zur Erhöhung der Sicherheit.

Aktivieren der Übereinstimmung mit Federal Information Processing Standard (FIPS) 140-2

Die vRealize Automation-Appliance verwendet jetzt die mit dem Federal Information Processing Standard (FIPS) 140-2 zertifizierte Version der OpenSSL-Bibliothek für die Datenübertragung über TLS für den gesamten eingehenden und ausgehenden Netzwerkdatenverkehr.

Sie können den FIPS-Modus in der Verwaltungsschnittstelle der vRealize Automation-Appliance aktivieren oder deaktivieren. Mit den folgenden Befehlen können Sie FIPS auch über die Befehlszeile konfigurieren, während Sie als Root-Benutzer angemeldet sind:

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Bei Aktivierung von FIPS verwendet der eingehende und ausgehende vRealize Automation-Appliance-Netzwerkverkehr an Port 443 eine FIPS 140-2-konforme Verschlüsselung. Unabhängig von der FIPS-Einstellung verwendet vRealize Automation AES-256, um gesicherte Daten zu schützen, die auf der vRealize Automation-Appliance gespeichert sind.

Hinweis Die FIPS-Übereinstimmung wird von vRealize Automation derzeit nur teilweise aktiviert, da einige interne Komponenten noch keine zertifizierten Verschlüsselungsmodule verwenden. In Fällen, in denen noch keine zertifizierten Module implementiert wurden, wird die AES-256-basierte Verschlüsselung in allen kryptografischen Algorithmen verwendet.

Hinweis Mithilfe des folgenden Verfahrens können Sie die physische Maschine neu starten, wenn Sie die Konfiguration ändern möchten.

Verfahren

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

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

- 2 Wählen Sie **vRA-Einstellungen > Hosteinstellungen** aus.
- 3 Klicken Sie oben rechts auf die Schaltfläche unter der Überschrift „Aktionen“, um FIPS zu aktivieren oder zu deaktivieren.
- 4 Klicken Sie auf **Ja**, um die vRealize Automation-Appliance neu zu starten.

Sicherstellen der Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1

Stellen Sie im Rahmen der Härtung sicher, dass die bereitgestellte vRealize Automation-Appliance sichere Übertragungskanäle verwendet.

Hinweis Nach dem Deaktivieren von TLS 1.0/1.1 und dem Aktivieren von TLS 1.2 können Sie den Vorgang zum Beitreten zum Cluster nicht mehr ausführen.

Voraussetzungen

Führen Sie [Aktivieren von TLS für die Localhost-Konfiguration](#) durch.

Verfahren

- 1 Stellen Sie die Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1 in den HAProxy-HTTP-Handlern auf der vRealize Automation-Appliance sicher.

Überprüfen Sie diese Datei	Stellen Sie sicher, dass folgender Inhalt	in der entsprechenden Zeile wie dargestellt vorhanden ist
/etc/haproxy/conf.d/20-vcac.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11
/etc/haproxy/conf.d/30-vro-config.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11

- 2 Starten Sie den Dienst neu.

```
service haproxy restart
```

- 3 Öffnen Sie die Datei /opt/vmware/etc/lighttpd/lighttpd.conf und stellen Sie sicher, dass die richtigen deaktivierten Einträge angezeigt werden.

Hinweis Es gibt keine Direktive zur Deaktivierung von TLS 1.0 oder TLS 1.1 in Lighttpd. Die Beschränkung für die Verwendung von TLS 1.0 und TLS 1.1 kann teilweise abgeschwächt werden, indem erzwungen wird, dass OpenSSL keine Verschlüsselungen von TLS 1.0 und TLS 1.1 verwendet.

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
```

- 4 Stellen Sie die Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1 für den Konsolenproxy auf der vRealize Automation-Appliance sicher.

- a Bearbeiten Sie die Datei `/etc/vcac/security.properties`, indem Sie die folgende Zeile hinzufügen oder ändern:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b Starten Sie den Server neu, indem Sie den folgenden Befehl ausführen:

```
service vcac-server restart
```

- 5 Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vCO-Dienst deaktiviert ist.

- a Suchen Sie das Tag `<Connector>` in der Datei `/etc/vco/app-server/server.xml` und fügen Sie das folgende Attribut hinzu:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Starten Sie den vCO-Dienst neu, indem Sie den folgenden Befehl ausführen.

```
service vco-server restart
```

- 6 Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vRealize Automation-Dienst deaktiviert ist.

- a Fügen Sie die folgenden Attribute zum Tag `<Connector>` in der Datei `/etc/vcac/server.xml` hinzu.

```
sslEnabledProtocols = "TLSv1.2"
```

- b Starten Sie den vRealize Automation-Dienst neu, indem Sie den folgenden Befehl ausführen:

```
service vcac-server restart
```

- 7 Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für RabbitMQ deaktiviert ist.

Öffnen Sie die Datei `/etc/rabbitmq/rabbitmq.config` und stellen Sie sicher, dass `{versions, ['tlsv1.2', 'tlsv1.1']}` in den Abschnitten „ssl“ und „ssl_options“ deaktiviert ist.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]}
  ]}
]
```

```

    ]},
    {mnesia_table_loading_timeout,600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].

```

- 8 Starten Sie den RabbitMQ-Server neu.

```
# service rabbitmq-server restart
```

- 9 Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vIDM-Dienst deaktiviert ist.

Öffnen Sie die Datei `opt/vmware/horizon/workspace/conf/server.xml` für jede Connector-Instanz, die `SSLEnabled="true"` enthält, und stellen Sie sicher, dass die folgende Zeile vorhanden ist.

```
sslEnabledProtocols="TLSv1.2"
```

Konfigurieren von TLS-Verschlüsselungs-Suites für vRealize Automation -Komponenten

Für maximale Sicherheit müssen Sie vRealize Automation-Komponenten für die Verwendung starker Verschlüsselungen konfigurieren.

Die zwischen dem Server und dem Browser ausgehandelte Verschlüsselungsschlüssel bestimmt die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird.

Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, deaktivieren Sie schwache Verschlüsselungen in vRealize Automation-Komponenten. Konfigurieren Sie den Server so, dass er nur starke Verschlüsselungen unterstützt und ausreichend große Schlüsselgrößen verwendet. Konfigurieren Sie außerdem alle Verschlüsselungen in einer geeigneten Reihenfolge.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites. Stellen Sie außerdem sicher, dass Verschlüsselungs-Suites, die den Diffie-Hellman (DHE)-Schlüsselaustausch verwenden, deaktiviert sind.

Deaktivieren von schwachen Verschlüsselungen im HA-Proxydienst

Überprüfen Sie die Verschlüsselungen im HA-Proxydienst für die vRealize Automation-Appliance anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Überprüfen Sie die Verschlüsselungseintrag der Bind-Direktive in der Datei `/etc/haproxy/conf.d/20-vcac.cfg` und deaktivieren Sie alle schwachen Verschlüsselungen.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls10 no-tls11
```

- 2 Überprüfen Sie die Verschlüsselungseintrag der Bind-Direktive in der Datei `/etc/haproxy/conf.d/30-vro-config.cfg` und deaktivieren Sie alle schwachen Verschlüsselungen.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls10 no-tls11
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance - Konsolenproxydienst der vRealize Automation -Appliance

Überprüfen Sie die Verschlüsselungen im Konsolenproxydienst der vRealize Automation-Appliance anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.
- 2 Fügen Sie eine Zeile zur Datei hinzu, um die unerwünschten Verschlüsselungen zu deaktivieren.

Verwenden Sie eine Variante der folgenden Zeile:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2 usw.
```

Um zum Beispiel die AES 128- und AES 256-Verschlüsselungen zu deaktivieren, fügen Sie die folgende Zeile hinzu:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Starten Sie den Server mit nachfolgend aufgeführtem Befehl neu.

```
service vcac-server restart
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance -vCO-Dienst

Überprüfen Sie die Verschlüsselungen im vRealize Automation-Appliance-vCO-Dienst anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Suchen Sie das Tag <Connector> in der Datei /etc/vco/app/server/server.xml.
- 2 Bearbeiten oder fügen Sie das Verschlüsselungsattribut hinzu, um die gewünschten Verschlüsselungs-Suites zu verwenden.

Informationen hierzu finden Sie im folgenden Beispiel:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance - RabbitMQ-Dienst

Überprüfen Sie die Verschlüsselungen im vRealize Automation-Appliance-RabbitMQ-Dienst anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Überprüfen Sie die unterstützten Verschlüsselungs-Suites, indem Sie den Befehl `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'` ausführen.

Die im folgenden Beispiel zurückgegebenen Verschlüsselungen stellen nur die unterstützten Verschlüsselungen dar. Der RabbitMQ-Server verwendet diese Verschlüsselungen nicht bzw. kündigt diese nicht an, es sei denn, diese Vorgehensweise ist in der Datei `rabbitmq.config` konfiguriert.

```
[ "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
  "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
  "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
  "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
  "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
  "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
  "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
  "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
  "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
  "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
  "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
  "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
  "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
  "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
  "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
  "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
  "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
  "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
  "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
  "ECDH-RSA-AES128-SHA", "AES128-SHA" ]
```

- 2 Wählen Sie die unterstützten Verschlüsselungen aus, die den Sicherheitsanforderungen Ihrer Organisation entsprechen.

Um beispielsweise nur `ECDHE-ECDSA-AES128-GCM-SHA256` & `ECDHE-ECDSA-AES256-GCM-SHA384` zuzulassen, überprüfen Sie die Datei `/etc/rabbitmq/rabbitmq.config` und fügen Sie die folgende Zeile unter `„ssl“` und `„ssl_options“` hinzu.

```
{ciphers, [ "ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384" ]}
```

- 3 Starten Sie den RabbitMQ-Server mithilfe des folgenden Befehls neu.

```
service rabbitmq-server restart
```

Überprüfen der Sicherheit von Data-at-Rest

Überprüfen Sie die Sicherheit der mit vRealize Automation verwendeten Datenbankbenutzer und -konten.

Postgres-Benutzer

Das Postgres-Linux-Benutzerkonto ist mit der Rolle des Postgres-Datenbankadministrators verknüpft und ist standardmäßig ein gesperrtes Konto. Dies ist die sicherste Konfiguration für diesen Benutzer, da der Zugriff nur über das Root-Benutzerkonto erfolgen kann. Entsperren Sie dieses Konto nicht.

Rollen für Datenbankbenutzerkonten

Die Standardrollen für Postgres-Benutzerkonten sollten nicht für Funktionen verwendet werden, bei denen es sich nicht um Anwendungsfunktionen handelt. Zur Unterstützung von nicht standardmäßigen Aktivitäten zur Datenbanküberprüfung und zur Erstellung von Datenbankberichten sollte ein zusätzliches Konto mit einem entsprechend geschützten Kennwort erstellt werden.

Führen Sie in der Befehlszeile das folgende Skript aus:

```
vcac-vami add-db-user newUsername newPassword
```

Hiermit wird ein neuer Benutzer und ein vom Benutzer angegebenes Kennwort hinzugefügt.

Hinweis Dieses Skript muss in den Fällen für die Master-Postgres-Datenbank ausgeführt werden, in denen ein Master-Slave-HA-Postgres-Setup konfiguriert ist.

Konfigurieren der PostgreSQL-Clientauthentifizierung

Stellen Sie sicher, dass die Authentifizierung der lokalen Vertrauensstellung nicht für die PostgreSQL-Datenbank der vRealize Automation-Appliance konfiguriert ist. Diese Konfiguration ermöglicht jedem lokalen Benutzer, einschließlich des Datenbankadministrators, ohne Kennwort eine Verbindung als PostgreSQL-Benutzer herzustellen.

Hinweis Für das Postgres-Superuser-Konto sollte eine lokale Vertrauensstellung beibehalten werden.

Die md5-Authentifizierungsmethode wird empfohlen, da sie verschlüsselte Kennwörter sendet.

Die Konfigurationseinstellungen der Clientauthentifizierung befinden sich in der Datei `/storage/db/pgdata/pg_hba.conf`.

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all postgres trust
# IPv4 local connections:
#host all all 127.0.0.1/32 md5
hostssl all all 127.0.0.1/32 md5
# IPv6 local connections:
#host all all ::1/128 md5
hostssl all all ::1/128 md5

# Allow remote connections for VCAC user.
#host vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac ::0/0 md5
# Allow remote connections for VCAC replication user.
#host vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication ::0/0 md5
```

```
# Allow replication connections by a user with the replication privilege.
#host    replication    vcac_replication    0.0.0.0/0    md5
hostssl  replication    vcac_replication    0.0.0.0/0    md5
hostssl  replication    vcac_replication    ::0/0        md5
```

Wenn Sie die Datei `pg_hba.conf` bearbeiten, müssen Sie den Postgres-Server neu starten, indem Sie die folgenden Befehle ausführen, bevor die Änderungen wirksam werden können.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Konfigurieren von vRealize Automation -Anwendungsressourcen

Überprüfen Sie die vRealize Automation-Anwendungsressourcen und beschränken Sie die Dateiberechtigungen.

Verfahren

- 1 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass Dateien mit SUID- und GUID-Bits ordnungsgemäß definiert sind.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Die folgende Liste wird angezeigt.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root    polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root    polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root    polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root    polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root    polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws--x--x  1 root    root       465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root    tty        10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x  1 root    root      142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x  1 root    shadow    161782 Sep 15  2015 /usr/bin/chage
2142467  156 -rwsr-xr-x  1 root    shadow    152850 Sep 15  2015 /usr/bin/chfn
1458298  364 -rwsr-xr-x  1 root    root      365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root    root       57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root    trusted   40432 Mar 18  2015 /usr/bin/crontab
2142478  148 -rwsr-xr-x  1 root    shadow    146459 Sep 15  2015 /usr/bin/chsh
2142480  156 -rwsr-xr-x  1 root    shadow    152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root    shadow    46967 Sep 15  2015 /usr/bin/expiry
311484  48 -rwsr-x---  1 root    messagebus 47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574  36 -rwsr-xr-x  1 root    shadow    35688 Apr 10  2014 /sbin/unix_chkpwd
876648  12 -rwsr-xr-x  1 root    shadow    10736 Dec 16  2011 /sbin/unix2_chkpwd
49308  68 -rwsr-xr-x  1 root    root      63376 May 27  2015 /opt/likewise/bin/ksu
```

```
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper
```

- 2 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass alle Dateien auf der virtuellen Appliance einen Besitzer haben.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Überprüfen Sie die Berechtigungen für alle Dateien auf der virtuellen Appliance, um sicherzustellen, dass keine von jedermann beschreibbar ist, indem Sie den folgenden Befehl ausführen.

```
find / -name "*.*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass nur der vCAC-Benutzer die richtigen Dateien besitzt.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Wenn keine Ergebnisse angezeigt werden, gehören alle Dateien nur dem vCAC-Benutzer.

- 5 Stellen Sie sicher, dass nur der vCAC-Benutzer Schreibrechte für die folgenden Dateien besitzt.

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

Überprüfen Sie außerdem die folgenden Dateien und deren Unterverzeichnisse:

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 6 Stellen Sie sicher, dass die richtigen Dateien in den folgenden Verzeichnissen und Unterverzeichnissen nur vom vCAC- oder Root-Benutzer gelesen werden können.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 7 Stellen Sie sicher, dass die richtigen Dateien nur im Besitz des vCO- oder Root-Benutzers sind, wie in den folgenden Verzeichnissen und deren Unterverzeichnissen dargestellt.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 8 Stellen Sie sicher, dass die richtigen Dateien nur vom vCO- oder Root-Benutzer beschrieben werden können, wie in den folgenden Verzeichnissen und Unterverzeichnissen dargestellt.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 9 Stellen Sie sicher, dass die richtigen Dateien nur vom vCO- oder Root-Benutzer gelesen werden können, wie in den folgenden Verzeichnissen und Unterverzeichnissen dargestellt.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

Anpassen der Konsolen-Proxykonfiguration

Sie können die Remote-Konsolenkonfiguration für vRealize Automation zur Erleichterung der Fehlerbehebung und organisatorischen Vorgehensweisen anpassen.

Wenn Sie vRealize Automation installieren, konfigurieren oder verwalten, können Sie einige Einstellungen ändern, um Fehlerbehebung und Debugging Ihrer Installation zu aktivieren. Katalogisieren und prüfen Sie alle vorgenommenen Änderungen, um sicherzustellen, dass anwendbare Komponenten entsprechend ihrer erforderlichen Verwendung korrekt abgesichert sind. Fahren Sie erst dann mit der Produktion fort, wenn Sie sicher sind, dass die Änderungen der Konfiguration korrekt abgesichert sind.

Anpassen des VMware Remote Console -Ticketablaufs

Sie können die Gültigkeitsdauer für Remote-Konsolen-Tickets, die für das Herstellen von VMware Remote Console-Verbindungen verwendet werden, anpassen.

Wenn ein Benutzer VMware Remote Console-Verbindungen herstellt, gibt das System neu erstellte, einmalige Anmeldedaten zurück, die eine bestimmte Verbindung zu einer virtuellen Maschine herstellen. Sie können den Ticketablauf für einen angegebenen Zeitraum in Minuten festlegen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.

- 2 Fügen Sie in der Datei eine Zeile im Format `consoleproxy.ticket.validitySec=30` hinzu.
Der numerische Wert in dieser Zeile gibt die Anzahl der Minuten an, bis das Ticket abläuft.
- 3 Speichern Sie die Datei und schließen Sie sie.
- 4 Starten Sie den vCAC-Server unter Verwendung des Befehls `/etc/init.d/vcac-server restart neu`.

Der Wert für den Ticketablauf wird auf den angegebenen Zeitraum in Minuten zurückgesetzt.

Anpassen des Konsolen-Proxyserver-Ports

Sie können den Port anpassen, auf dem der VMware Remote Console-Konsolenproxy Nachrichten empfängt.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.
- 2 Fügen Sie in der Datei eine Zeile im Format `consoleproxy.service.port=8445` hinzu.
Der numerische Wert gibt die Nummer des Konsolen-Proxydienst-Ports an, die in diesem Fall 8445 ist.
- 3 Speichern Sie die Datei und schließen Sie sie.
- 4 Starten Sie den vCAC-Server unter Verwendung des Befehls `/etc/init.d/vcac-server restart neu`.

Der Proxydienst-Port wird in die angegebene Portnummer geändert.

Konfigurieren der X-XSS-Schutz-Antwortkopfzeile

Fügen Sie die X-XSS-Schutz-Antwortkopfzeile der haproxy-Konfigurationsdatei hinzu.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.
- 2 Fügen Sie die folgenden Zeilen in einem Front-End-Abschnitt hinzu:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
      rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.
`/etc/init.d/haproxy reload`

Konfigurieren der HTTP Strict Transport Security-Antwortkopfzeile

Fügen Sie die HTTP Strict Transport Security(HSTS)-Antwortkopfzeile der HAProxy-Konfiguration hinzu.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.

- 2 Fügen Sie die folgenden Zeilen in einem Front-End-Abschnitt hinzu:

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.

```
/etc/init.d/haproxy reload
```

Konfigurieren der X-Frame-Options-Antwortkopfzeile

Die X-Frame-Options-Antwortkopfzeile wird möglicherweise in einigen Fällen zweimal angezeigt.

Die X-Frame-Options-Antwortkopfzeile wird möglicherweise zweimal angezeigt, da der vIDM-Dienst diese Kopfzeile dem Back-End sowie HAProxy hinzufügt. Sie können mit einer entsprechenden Konfiguration verhindern, dass er zweimal angezeigt wird.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.

- 2 Suchen Sie die folgende Zeile im Front-End-Abschnitt:

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

- 3 Fügen Sie die folgenden Zeilen vor der Zeile ein, die Sie im vorherigen Schritt ermittelt haben:

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

- 4 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.

```
/etc/init.d/haproxy reload
```

Konfigurieren von Server-Antwortkopfzeilen

Aus Sicherheitsgründen wird die Konfiguration Ihres vRealize Automation-Systems zur Beschränkung der für potenzielle Angreifer verfügbaren Informationen empfohlen.

Minimieren Sie die Menge der Informationen soweit wie möglich, die Ihr System über seine Identität und Version offen legt. Hacker und Kriminelle können diese Informationen für zielgerichtete Angriffe auf Ihren Webserver verwenden.

Konfigurieren der Lighttpd-Server-Antwortkopfzeile

Erstellen Sie als Best Practice eine leere Serverkopfzeile für den lighttpd-Server der vRealize Automation-Apliance.

Verfahren

- 1 Öffnen Sie die Datei `/opt/vmware/etc/lighttpd/lighttpd.conf` in einem Texteditor.

- 2 Fügen Sie `server.tag = " "` der Datei hinzu.

- 3 Speichern Sie die Änderungen und schließen Sie die Datei.

- 4 Starten Sie den lighttpd-Server durch Ausführen des Befehls `# /opt/vmware/etc/init.d/vami-lighttpd restart neu`.

Konfigurieren der TCServer-Antwortkopfzeile für die vRealize Automation -Appliance

Erstellen Sie als Best Practice eine benutzerdefinierte leere Serverkopfzeile für die TCServer-Antwortkopfzeile, die mit der vRealize Automation-Appliance verwendet wird, um die Möglichkeit bössartiger Angreifer einzuschränken, an wertvolle Informationen zu gelangen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vco/app-server/server.xml` in einem Texteditor.
- 2 Hinzufügen von `server=""` in jedem `<Connector>`-Element
Beispiel: `<Connector protocol="HTTP/1.1" server="" />`
- 3 Speichern Sie die Änderungen und schließen Sie die Datei.
- 4 Starten Sie den Server mit nachfolgend aufgeführtem Befehl neu.

```
service vco-server restart
```

Konfigurieren der Antwortkopfzeile des Internet Information Services-Servers

Erstellen Sie als Best Practice eine benutzerdefinierte leere Serverkopfzeile für den Internet Information Services(IIS)-Server, die mit der Identity Appliance verwendet wird, um die Möglichkeit bössartiger Angreifer einzuschränken, an wertvolle Informationen zu gelangen.

Verfahren

- 1 Öffnen Sie die Datei `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` in einem Texteditor.
- 2 Suchen Sie nach `RemoveServerHeader=0` und ändern Sie den Ausdruck in `RemoveServerHeader=1..`
- 3 Speichern Sie die Änderungen und schließen Sie die Datei.
- 4 Führen Sie den Befehl `iisreset` aus, um den Server neu zu starten.

Nächste Schritte

Deaktivieren Sie die IIS X-Powered By-Kopfzeile, indem Sie HTTP-Antwortkopfzeilen aus der Liste in der IIS-Manager-Konsole entfernen.

- 1 Öffnen Sie die IIS-Manager-Konsole.
- 2 Öffnen Sie die HTTP-Antwortkopfzeile und entfernen Sie sie aus der Liste.
- 3 Führen Sie den Befehl `iisreset` aus, um den Server neu zu starten.

Festlegen der Zeitüberschreitung für eine vRealize Automation-Appliance -Sitzung

Konfigurieren Sie den Zeitüberschreitungswert für die Sitzung auf der vRealize Automation-Appliance gemäß den Sicherheitsrichtlinien Ihres Unternehmens.

Der standardmäßige Zeitüberschreitungswert bei Inaktivität für eine vRealize Automation-Appliance-Sitzung beträgt 30 Minuten. Um diesen Wert gemäß den Sicherheitsrichtlinien Ihres Unternehmens anzupassen, bearbeiten Sie die Datei `web.xml` auf Ihrer vRealize Automation-Appliance-Hostmaschine.

Verfahren

- 1 Öffnen Sie die Datei `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` in einem Texteditor.
- 2 Suchen Sie den Eintrag `session-config` und legen Sie den Wert für Zeitüberschreitung der Sitzung fest. Schauen Sie sich das folgende Codebeispiel an.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Starten Sie den Server neu, indem Sie den folgenden Befehl ausführen.

```
service vcac-server restart
```

Verwalten nicht erforderlicher Software

Um Sicherheitsrisiken zu minimieren, entfernen Sie nicht erforderliche Software von Ihren vRealize Automation-Hostmaschinen.

Konfigurieren Sie jegliche Software, die Sie nicht gemäß den Empfehlungen des Herstellers und den Best Practices zur Sicherheit entfernen, um die Gefahr von Sicherheitsverstößen zu minimieren.

Sichern des USB-Massenspeicher-Handlers

Sichern Sie den USB-Massenspeicher-Handler, um dessen Verwendung als USB-Geräte-Handler mit Hostmaschinen der virtuellen VMware-Appliances zu verhindern. Potenzielle Angreifer können diesen Handler ausnutzen, um Ihr System zu gefährden.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die `install usb-storage /bin/true`-Zeile in der Datei angezeigt wird.
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des Bluetooth-Protokoll-Handlers

Sichern Sie den Bluetooth-Protokoll-Handler auf den Hostmaschinen Ihrer virtuellen Appliances, um potenzielle Angriffe zu verhindern.

Das Binden des Bluetooth-Protokolls an den Netzwerkstapel ist nicht erforderlich und kann den Host für Angriff anfälliger machen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.

- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install bluetooth /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des SCTP (Stream Control Transmission Protocol)-Protokolls

Verhindern Sie, dass das SCTP-Protokoll standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Konfigurieren Sie Ihr System, um zu verhindern, dass das SCTP-Modul geladen wird, sofern dies nicht absolut notwendig ist. SCTP ist ein nicht verwendetes, durch IETF standardisiertes Transportebenenprotokoll. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechtigte lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er ein Socket mit dem Protokoll öffnet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install sctp /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des DCCP (Datagram Congestion Protocol)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das DCCP-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des DCCP-Moduls, sofern dies nicht absolut notwendig ist. DCCP ist ein vorgeschlagenes Transportebenenprotokoll, das nicht verwendet wird. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechtigte lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die DCCP-Zeilen in der Datei angezeigt werden.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern der Netzwerküberbrückung

Verhindern Sie, dass das Netzwerküberbrückungs-Modul standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können diese Überbrückung ausnutzen, um Ihr System zu gefährden.

Konfigurieren Sie Ihr System, um zu verhindern, dass das Netzwerk geladen wird, sofern dies nicht absolut notwendig ist. Potenzielle Angreifer können diese Schwachstelle ausnutzen, um die Netzwerkpartitionierung und -sicherheit zu umgehen.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der virtuellen VMware-Appliances aus.

```
# rmmmod bridge
```

- 2 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 3 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install bridge /bin/false
```

- 4 Speichern Sie die Datei und schließen Sie sie.

Sichern des RDS (Reliable Datagram Sockets)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das RDS-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Wenn Sie das RDS-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die Zeile `install rds /bin/true` angezeigt wird.
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des TIPC (Transparent Inter-Process Communication)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das TIPC-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Wenn Sie das TIPC-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die Zeile `install tipc /bin/true` angezeigt wird.
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des IPX (Internetwork Packet Exchange)-Protokolls

Verhindern Sie, dass das IPX-Protokoll standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des IPX-Protokollmoduls, sofern dies nicht absolut notwendig ist. Das IPX-Protokoll ist ein veraltetes Netzwerkschichtprotokoll. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install ipx /bin/true
```
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des AppleTalk-Protokolls

Verhindern Sie, dass das AppleTalk-Protokoll standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des AppleTalk-Protokolls, sofern dies nicht absolut notwendig ist. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install appletalk /bin/true
```
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des DECnet-Protokolls

Verhindern Sie, dass das DECnet-Protokoll standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des DECnet-Protokollmoduls, sofern dies nicht absolut notwendig ist. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die `/etc/modprobe.conf.local`-Datei für das DECnet-Protokoll in einem Texteditor.

- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install decnet /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des Firewire-Moduls

Verhindern Sie, dass das Firewire-Modul standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des Firewire-Moduls, sofern dies nicht absolut notwendig ist.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install ieee1394 /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern der Infrastructure as a Service-Komponente

Wenn Sie Ihr System härten, sichern Sie die vRealize Automation Infrastructure as a Service (IaaS)-Komponente und die jeweilige Hostmaschine, um potenzielle Angriffe zu verhindern.

Sie müssen eine Sicherheitseinstellung für die vRealize Automation Infrastructure as a Service (IaaS)-Komponente und den jeweiligen Host konfigurieren. Sie müssen die Konfiguration von anderen zugehörigen Komponenten und Anwendungen festlegen bzw. überprüfen. In einigen Fällen können Sie die vorhandenen Einstellungen übernehmen, in anderen hingegen müssen Sie Einstellungen für eine entsprechende Konfiguration ändern bzw. hinzufügen.

Deaktivieren des Windows-Zeitdiensts

Aus Sicherheitsgründen wird in einer vRealize Automation-Produktionsumgebung die Verwendung von autorisierten Zeitservern anstelle der Host-Uhrzeitsynchronisierung empfohlen.

Deaktivieren Sie in einer Produktionsumgebung die Host-Uhrzeitsynchronisierung und verwenden Sie autorisierte Zeitserver, um die präzise Verfolgung von Benutzeraktionen sowie die Identifizierung von möglicherweise böswilligen Angriffen und das Eindringen durch Überwachung und Protokollierung zu unterstützen.

Konfigurieren von TLS für Infrastructure as a Service-Data-In-Transit

Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung starke TLS-Protokolle verwendet, um Übertragungskanäle für Infrastructure as a Service-Komponenten zu sichern.

Secure Sockets Layer (SSL) und das neuere Transport Layer Security (TLS) sind kryptografische Protokolle, die die Sicherheit des Systems während der Netzwerkkommunikation zwischen verschiedenen Systemkomponenten sicherstellen. Da SSL ein älterer Standard ist, bieten viele seiner Implementierungen keine ausreichende Sicherheit vor potenziellen Angriffen mehr. Bei früheren SSL-Protokollen einschließlich SSLv2 und SSLv3 wurden schwerwiegende Schwächen identifiziert. Diese Protokolle werden nicht mehr als sicher erachtet.

Je nach den Sicherheitsrichtlinien Ihrer Organisation ist es möglicherweise auch ratsam, TLS 1.0 zu deaktivieren.

Hinweis Beim Beenden von TLS auf dem Lastausgleichsdienst können Sie auch unsichere Protokolle wie SSLv2, SSLv3 sowie TLS 1.0 falls erforderlich deaktivieren.

Deaktivieren von SSLv3 in Internetinformationsdienste

Die Deaktivierung von SSLv3 in Internetinformationsdienste (Internet Information Services, IIS) auf der IaaS (Infrastructure as a Service)-Maschine hat sich aus Sicherheitsgründen sehr bewährt.

Verfahren

- 1 Führen Sie den Registrierungs-Editor von Windows als Administrator aus.
- 2 Navigieren Sie im Registrierungsfenster zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\.
- 3 Klicken Sie mit der rechten Maustaste auf **Protokolle** und wählen Sie **Neu > Schlüssel** aus.
- 4 Geben Sie **SSL 3.0** ein.
- 5 Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den neu erstellten **SSL 3.0-Schlüssel**, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie **Client** ein.
- 6 Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den neu erstellten **SSL 3.0-Schlüssel**, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie die **Server** ein.
- 7 Klicken Sie in der Navigationsstruktur unter „SSL 3.0“ mit der rechten Maustaste auf **Client**, wählen Sie **Neu > DWORD-Wert (32-Bit)** aus und geben Sie **DisabledByDefault** ein.
- 8 Wählen Sie in der Navigationsstruktur unter „SSL 3.0“ die Option **Client** aus, doppelklicken Sie im rechten Fensterbereich auf **DisabledByDefault** und geben Sie **1** ein.
- 9 Klicken Sie in der Navigationsstruktur unter „SSL 3.0“ mit der rechten Maustaste auf **Server**, wählen Sie **Neu > DWORD-Wert (32-Bit)** aus und geben Sie **Enabled** ein.
- 10 Wählen Sie in der Navigationsstruktur unter „SSL 3.0“ die Option **Server** aus, doppelklicken Sie im rechten Bereich auf den aktivierten Wert **DWORD** und geben Sie **0** ein.
- 11 Starten Sie den Windows-Server neu.

Deaktivieren von TLS 1.0 für IaaS

Um maximale Sicherheit zu bieten, konfigurieren Sie IaaS zur Verwendung von Pooling und deaktivieren Sie TLS 1.0.

Weitere Informationen finden Sie im Microsoft-Knowledgebase-Artikel unter <https://support.microsoft.com/en-us/kb/245030>.

Verfahren

- 1 Konfigurieren Sie IaaS zur Verwendung von Pooling anstelle von Web-Sockets.
 - a Aktualisieren Sie die Manager Services-Konfigurationsdatei C:\Programme (x86)\VMware\re\VCAC\Server\ManagerService.exe.config, indem Sie die folgenden Werte im <appSettings>-Abschnitt hinzufügen.

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

- b Starten Sie den Manager Service (VMware vCloud Automation Center Service) neu.
- 2 Vergewissern Sie sich, dass TLS 1.0 auf dem IaaS-Server deaktiviert ist.
 - a Führen Sie den Registrierungs-Editor als Administrator aus.
 - b Navigieren Sie im Registrierungsfenster zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\.
 - c Klicken Sie mit der rechten Maustaste auf „Protokolle“, wählen Sie **Neu > Schlüssel** aus und geben Sie **TLS 1.0** ein.
 - d Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den TLS 1.0-Schlüssel, den Sie gerade erstellt haben, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie **Client** ein.
 - e Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den TLS 1.0-Schlüssel, den Sie gerade erstellt haben, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie **Server** ein.
 - f Klicken Sie in der Navigationsstruktur unter „TLS 1.0“ mit der rechten Maustaste auf **Client**, klicken Sie auf **Neu > DWORD-Wert (32-Bit)** und geben Sie **DisabledByDefault** ein.
 - g Wählen Sie in der Navigationsstruktur unter „TLS 1.0“ die Option **Client** aus, doppelklicken Sie im rechten Bereich auf **DisabledByDefault** DWORD und geben Sie **1** ein.
 - h Klicken Sie in der Navigationsstruktur unter „TLS 1.0“ mit der rechten Maustaste auf **Server**, wählen Sie **Neu > DWORD-Wert (32-Bit)** aus und geben Sie **Enabled** ein.
 - i Wählen Sie in der Navigationsstruktur unter „TLS 1.0“ die Option **Server** aus, doppelklicken Sie im rechten Bereich auf das DWORD **Aktiviert** und geben Sie **0** ein.
 - j Starten Sie den Windows-Server neu.

Konfigurieren von TLS-Verschlüsselungs-Suites

Für maximale Sicherheit müssen Sie vRealize Automation-Komponenten für die Verwendung starker Verschlüsselungen konfigurieren. Die zwischen dem Server und dem Browser ausgehandelte Verschlüsselungsschlüssel bestimmt die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird. Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, deaktivieren Sie schwache Verschlüsselungen in vRealize Automation-Komponenten. Konfigurieren Sie den Server so, dass er nur starke Verschlüsselungen unterstützt und ausreichend große Schlüsselgrößen verwendet. Konfigurieren Sie außerdem alle Verschlüsselungen in einer geeigneten Reihenfolge.

Nicht akzeptable Verschlüsselungs-Suites

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites. Stellen Sie außerdem sicher, dass Verschlüsselungs-Suites, die den Diffie-Hellman (DHE)-Schlüsselaustausch verwenden, deaktiviert sind.

Überprüfen der Hostserver-Sicherheit

Aus Sicherheitsgründen wird empfohlen, die Konfiguration der Sicherheit auf Ihren IaaS (Infrastructure as a Service)-Hostserver-Maschinen zu überprüfen.

Microsoft bietet verschiedene Tools zum Überprüfen der Sicherheit auf Hostserver-Maschinen. Hilfestellung für den Einsatz dieser Tools erhalten Sie von Ihrem Microsoft-Anbieter.

Überprüfen der sicheren Baseline für Hostserver

Mit dem Microsoft Baseline Security Analyzer (MBSA) können Sie schnell feststellen, ob Ihr Server über die neuesten Aktualisierungen oder Hotfixes verfügt. Sie können den MBSA zum Installieren von fehlenden Microsoft-Sicherheitspatches verwenden, um Ihren Server mit den neuesten Sicherheitsempfehlungen von Microsoft auf dem neuesten Stand zu halten.

Laden Sie die neueste Version des MBSA-Tools von der Microsoft-Website herunter.

Überprüfen der Sicherheitskonfiguration der Hostserver

Verwenden Sie den Windows-Sicherheitskonfigurations-Assistenten (Windows Security Configuration Wizard, SCW) und das Microsoft Security Compliance Manager (SCM)-Toolkit, um sicherzustellen, dass der Hostserver sicher konfiguriert ist.

Führen Sie den SCW unter Verwendung des Verwaltungstools Ihres Windows-Servers aus. Mit diesem Tool können die Rollen Ihres Servers sowie die installierten Funktionen, einschließlich Netzwerk, Windows-Firewalls und Registrierungseinstellungen, identifiziert werden. Vergleichen Sie den Bericht mit den aktuellen Anweisungen zur Härtung aus dem entsprechenden SCM für Ihren Windows-Server. Basierend auf den Ergebnissen können Sie eine Feinabstimmung der Sicherheitseinstellungen für jede Funktion vornehmen (wie zum Beispiel für Netzwerkdienste, Kontoeinstellungen und Windows-Firewalls) und die Einstellungen auf Ihren Server anwenden.

Weitere Informationen zum SCW-Tool finden Sie auf der Microsoft Technet-Website.

Schützen von Anwendungsressourcen

Stellen Sie aus Sicherheitsgründen sicher, dass alle relevanten Infrastructure as a Service-Dateien über die entsprechenden Berechtigungen verfügen.

Überprüfen Sie Infrastructure as a Service-Dateien in Ihrer Infrastructure as a Service-Installation. In den meisten Fällen stimmen die Unterordner und Dateien für alle Ordner mit den Einstellungen des Ordners überein.

Verzeichnis oder Datei	Gruppe oder Benutzer	Vollständige Kontrolle	Ändern	Lesen und ausführen	Lesen	Schreiben
VMware\<agent_name>\logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\<agent_name>\temp	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\<agent_name>\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\<agent_name>\Distributed Execution Manager\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\<agent_name>\Distributed Execution Manager\DEM\Logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\<agent_name>\Distributed Execution Manager\DEO\Logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\<agent_name>\Management Agent\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X

Verzeichnis oder Datei	Gruppe oder Benutzer	Vollständige Kontrolle		Lesen und ausführen		Schreiben
		Ändern		Lesen		
VMware\VCAC\Server\	Benutzer			X	X	
	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\VCAC\Web API	Benutzer			X	X	
	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	

Sichern der Infrastructure as a Service-Hostmaschine

Überprüfen Sie als Best Practice im Hinblick auf die Sicherheit die allgemeinen Einstellungen auf Ihrer Infrastructure as a Service (IaaS)-Hostmaschine, um sicherzustellen, dass sie den Sicherheitsrichtlinien entspricht.

Sichern Sie sonstige Konten, Anwendungen, Ports und Dienste auf der Infrastructure as a Service (IaaS)-Hostmaschine.

Überprüfen der Benutzerkontoeinstellungen des Servers

Stellen Sie sicher, dass keine unnötigen lokalen und Domänenbenutzerkonten und -Einstellungen vorhanden sind. Beschränken Sie alle Benutzerkonten, die nicht im Zusammenhang mit den Funktionen der Anwendung stehen, auf diejenigen, die für die Verwaltung, Wartung und Fehlerbehebung erforderlich sind. Beschränken Sie den Remotezugriff über Domänenbenutzerkonten auf das erforderliche Mindestmaß für die Wartung des Servers. Kontrollieren und prüfen Sie diese Konten genau.

Löschen unnötiger Anwendungen

Löschen Sie alle nicht benötigten Anwendungen von den Hostservern. Nicht benötigte Anwendungen erhöhen das Risiko einer Offenlegung aufgrund ihrer unbekannt oder unbehobenen Schwachstellen.

Deaktivieren unnötiger Ports und Dienste

Überprüfen Sie die Hostserver-Firewall auf die Liste offener Ports. Blockieren Sie alle Ports, die für die IaaS-Komponente oder den kritischen Systemvorgang nicht erforderlich sind. Siehe [Konfigurieren von Ports und Protokollen](#). Überwachen Sie die Dienste, die für Ihren Hostserver ausgeführt werden, und deaktivieren Sie all jene, die nicht benötigt werden.

Konfigurieren der Hostnetzwerksicherheit

Um maximalen Schutz vor bekannten Sicherheitsrisiken zu ermöglichen, konfigurieren Sie Einstellungen für die Netzwerkschnittstelle und Kommunikation auf allen VMware-Hostmaschinen.

Konfigurieren Sie im Rahmen eines umfassenden Sicherheitsplans die Einstellungen für die Sicherheit der Netzwerkschnittstelle für die virtuellen VMware-Appliances und die Infrastructure as a Service-Komponenten gemäß den festgelegten Sicherheitsrichtlinien.

Konfigurieren von Netzwerkeinstellungen für VMware -Appliances

Um sicherzustellen, dass die Hostmaschinen der virtuellen VMware-Appliance nur sichere und wichtige Kommunikation unterstützen, überprüfen und bearbeiten Sie deren Einstellungen für die Netzwerkkommunikation.

Überprüfen Sie die Netzwerk-IP-Protokollkonfiguration der VMware-Hostmaschine und konfigurieren Sie die Netzwerkeinstellungen gemäß den Sicherheitsrichtlinien. Deaktivieren Sie alle nicht benötigten Kommunikationsprotokolle.

Verhindern der Benutzerkontrolle von Netzwerkschnittstellen

Aus Sicherheitsgründen wird empfohlen, Benutzern nur die Systemberechtigungen zu gewähren, die sie für ihre Arbeit auf den Hostmaschinen der VMware-Appliances benötigen.

Das Zulassen der Bearbeitung von Netzwerkschnittstellen durch Benutzerkonten kann zur Umgehung von Sicherheitsmechanismen für das Netzwerk oder zum Denial-of-Service führen. Beschränken Sie das Ändern der Einstellungen von Netzwerkschnittstellen auf berechtigte Benutzer.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der VMware-Appliances aus.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Stellen Sie sicher, dass jede Schnittstelle auf NO festgelegt ist.

Festlegen der Warteschlangengröße für TCP-Backlogs

Um eine bestimmte Verteidigungsebene gegen Angriffe bereitzustellen, konfigurieren Sie eine Standardwarteschlangengröße für TCP-Backlogs auf den Hostmaschinen der VMware-Appliances.

Legen Sie die Warteschlangengröße für TCP-Backlogs auf einen entsprechenden Standardwert fest, um das Risiko von TCP-Denial-of-Service-Angriffen zu minimieren. Die empfohlene Standardeinstellung ist 1280.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der VMware-Appliances durch.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Öffnen Sie die Datei `/etc/sysctl.conf` mit einem Texteditor.
- 3 Legen Sie die Standardwarteschlangengröße für TCP-Backlogs fest, indem Sie der Datei den folgenden Eintrag hinzufügen.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern von ICMPv4-Echos für Broadcast-Adressen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der VMware-Appliance Anforderungen für ICMP-Broadcast-Adressen-Echos ignorieren.

Antworten auf Broadcast-Internet Control Message Protocol (ICMP)-Echos bieten einen Angriffspunkt für Verstärkungsangriffe und können die Netzwerkzuordnung durch bösartige Agents erleichtern. Wenn Sie die Hostmaschinen der Appliance so konfigurieren, dass ICMPv4-Echos ignoriert werden, wird ein Schutz vor solchen Angriffen geboten.

Verfahren

- 1 Führen Sie den `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`-Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um zu bestätigen, dass sie Anforderungen für IPv4-Broadcast-Adressen-Echos ablehnen.

Wenn die Hostmaschinen für die Ablehnung von IPv4-Umleitungen konfiguriert sind, gibt dieser Befehl einen Wert von 0 für `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` zurück.

- 2 Um die Hostmaschine einer virtuellen Appliance für die Ablehnung von Anforderungen für ICMPv4-Broadcast-Adressen-Echos zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` auf Windows-Hostmaschinen in einem Texteditor.
- 3 Suchen Sie nach dem Eintrag `net.ipv4.icmp_echo_ignore_broadcasts=0`. Wenn der Wert für diesen Eintrag nicht auf 0 gesetzt oder der Eintrag nicht vorhanden ist, fügen Sie ihn hinzu oder aktualisieren den vorhandenen Eintrag entsprechend.
- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Deaktivieren von IPv4 Proxy ARP

Stellen Sie sicher, dass IPv4 Proxy ARP deaktiviert ist, falls die Aktivierung auf den Hostmaschinen Ihrer VMware-Appliance nicht erforderlich ist, um die nicht autorisierte Freigabe von Informationen zu verhindern.

Mit IPv4 Proxy ARP kann ein System Antworten auf ARP-Anfragen im Namen von verbundenen Hosts von einer Schnittstelle an eine andere Schnittstelle senden. Deaktivieren Sie die Funktion, falls nicht erforderlich, um die Weitergabe von Adressinformationen zwischen den angehängten Netzwerksegmenten zu verhindern.

Verfahren

- 1 Führen Sie den `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"`-Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um sicherzustellen, dass IPv4 Proxy ARP deaktiviert ist.

Wenn auf den Hostmaschinen IPv6 Proxy ARP deaktiviert ist, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie IPv6 Proxy ARP auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

3 Überprüfen Sie die folgenden Einträge.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv4-ICMP-Umleitungsmeldungen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der virtuellen VMware-Appliance IPv4-ICMP-Umleitungsmeldungen ablehnen.

Router verwenden ICMP-Umleitungsmeldungen, um Hosts mitzuteilen, dass für ein Ziel eine direktere Route vorhanden ist. Eine bösartige ICMP-Umleitungsmeldung kann einen Man-in-the-Middle-Angriff erleichtern. Diese Meldungen ändern die Routentabelle des Hosts und sind nicht authentifiziert. Stellen Sie sicher, dass das System so konfiguriert ist, dass diese ignoriert werden, wenn sie ansonsten nicht benötigt werden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie IPv4-Umleitungsmeldungen verweigern.

Dieser Befehl gibt Folgendes zurück, wenn die Hostmaschinen für die Verweigerung von IPv4-Umleitungsmeldungen konfiguriert sind:

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Wenn Sie eine Hostmaschine der virtuellen Appliance für die Verweigerung von IPv4-Umleitungsmeldungen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt sind oder wenn die Einträge nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Speichern Sie die von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-ICMP-Umleitungsmeldungen

Stellen Sie als Best Practice für Sicherheit sicher, dass die Hostmaschinen Ihrer virtuellen VMware-Appliance IPv6-ICMP-Umleitungsmeldungen verweigern.

Router verwenden ICMP-Umleitungsmeldungen, um Hosts mitzuteilen, dass für ein Ziel eine direktere Route vorhanden ist. Eine bösartige ICMP-Umleitungsmeldung kann einen Man-in-the-Middle-Angriff erleichtern. Diese Meldungen ändern die Routentabelle des Hosts und sind nicht authentifiziert. Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass diese Meldungen ignoriert werden (falls nicht anderweitig erforderlich).

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` auf den Hostmaschinen der virtuellen VMware-Appliance aus, um zu bestätigen, dass IPv6-Umleitungsmeldungen verweigert werden.

Wenn die Hostmaschinen für die Verweigerung von IPv6-Umleitungsmeldungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Um eine Hostmaschine der virtuellen Appliance zum Verweigern von IPv4-Umleitungsmeldungen zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv6.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt oder die Einträge nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Protokollieren von IPv4-Martian-Paketen

Stellen Sie als Best Practice für Sicherheit sicher, dass die Hostmaschinen Ihrer virtuellen VMware-Appliance IPv4-Martian-Pakete protokollieren.

Martian-Pakete enthalten Adressen, die das System als ungültig erkennt. Konfigurieren Sie Ihre Hostcomputer zur Protokollierung dieser Meldungen, damit Sie falsche Konfigurationen oder laufende Angriffe identifizieren können.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass IPv4-Martian-Pakete protokolliert werden.

Wenn die virtuellen Maschinen zum Konfigurieren von Martian-Paketen konfiguriert sind, geben sie Folgendes zurück:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie die virtuellen Maschinen zum Konfigurieren von IPv4-Martian-Paketen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn der Wert der folgenden Einträge nicht auf 1 gesetzt ist oder die Werte nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verwenden der IPv4 Reverse Path-Filterung

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der virtuellen VMware-Appliance IPv4 Reverse Path-Filterung verwenden.

Reverse Path-Filterung schützt vor manipulierten Quelladressen, indem das System Pakete mit Quelladressen verwirft, die über keine Route oder eine Route verfügen, die nicht auf die ursprüngliche Schnittstelle verweist. Konfigurieren Sie Ihre Hostmaschinen für die Verwendung von Reverse Path-Filterung wann immer möglich. In einigen Fällen, je nach Systemrolle, kann Reverse Path-Filterung bewirken, dass das System legitimen Datenverkehr verwirft. Wenn solche Probleme auftreten, müssen Sie möglicherweise einen weniger strengen Modus verwenden oder Reverse Path-Filterung vollständig deaktivieren.

Verfahren

- 1 Führen Sie den `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | grep "default|all"`-Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um sicherzustellen, dass IPv4 Reverse Path-Filterung verwendet wird.

Dieser Befehl gibt Folgendes zurück, wenn die virtuellen Maschinen IPv4 Reverse Path-Filterung verwenden:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

Wenn Ihre virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie IPv4 Reverse Path-Filterung auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf 1 gesetzt oder nicht vorhanden sind, fügen Sie sie der Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv4-Weiterleitung

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance die IPv4-Weiterleitung verweigern.

Wenn das System für die IP-Weiterleitung konfiguriert ist und kein designierter Router ist, könnten Angreifer es nutzen, um die Netzwerksicherheit zu umgehen, indem sie einen Pfad für die Kommunikation, die nicht von Netzwerkgeräten gefiltert wird, bereitstellen. Konfigurieren Sie die Hostmaschinen der virtuellen Appliance so, dass die IPv4-Weiterleitung verweigert wird, um dieses Risiko zu vermeiden.

Verfahren

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/ip_forward` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie die IPv4-Weiterleitung verweigern.

Wenn die Hostmaschinen so konfiguriert sind, dass sie die IPv4-Weiterleitung verweigern, gibt dieser Befehl einen Wert von 0 für `/proc/sys/net/ipv4/ip_forward` zurück. Wenn die virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Um die Hostmaschine der virtuellen Appliance für das Verweigern der IPv4-Weiterleitung zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Suchen Sie nach dem Eintrag `net.ipv4.ip_forward=0`. Wenn der Wert für diesen Eintrag derzeit nicht auf Null gesetzt ist oder wenn der Eintrag nicht vorhanden ist, fügen Sie ihn hinzu oder aktualisieren Sie den vorhandenen Eintrag entsprechend.
- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv6-Weiterleitung

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die VMware-Appliance-Hostsysteme die IPv6-Weiterleitung verweigern.

Wenn das System für die IP-Weiterleitung konfiguriert ist und kein designierter Router ist, könnten Angreifer es nutzen, um die Netzwerksicherheit zu umgehen, indem sie einen Pfad für die Kommunikation, die nicht von Netzwerkgeräten gefiltert wird, bereitstellen. Konfigurieren Sie die Hostmaschinen der virtuellen Appliance für die Verweigerung der IPv6-Weiterleitung, um dieses Risiko zu vermeiden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die IPv6-Weiterleitung ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Weiterleitung konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der IPv6-Weiterleitung konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv6.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt sind oder wenn die Einträge nicht vorhanden sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verwenden von IPv4-TCP Syncookies

Stellen Sie sicher, dass die Hostmaschinen Ihrer VMware-Appliance IPv4-TCP Syncookies verwenden.

Ein TCP SYN-Flutangriff führt möglicherweise zu einem Denial-of-Service, indem die TCP-Verbindungstabelle eines Systems mit Verbindungen im SYN_RCVD-Status aufgefüllt wird. Syncookies verhindern das Nachverfolgen einer Verbindung bis zum Erhalt einer nachfolgenden Quittierung und stellen sicher, dass der Initiator eine gültige Verbindung herstellt und keine Flutquelle ist. Dieses Verfahren funktioniert nicht in einer vollständigen Übereinstimmung mit den Standards. Es wird daher nur während einer Flutbedingung eingesetzt und ermöglicht die Absicherung des Systems bei fortwährender Verarbeitung von Anforderungen.

Verfahren

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/tcp_syncookies` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass IPv4-TCP Syncookies verwendet werden.

Wenn die Hostmaschinen zum Ablehnen der IPv4-Weiterleitung konfiguriert sind, gibt dieser Befehl einen Wert von 1 für `/proc/sys/net/ipv4/tcp_syncookies` zurück. Wenn die virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine virtuelle Appliance zur Verwendung von IPv4-TCP Syncookies konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

- 3 Suchen Sie nach dem Eintrag `net.ipv4.tcp_syncookies=1`.

Wenn der Wert für diesen Eintrag aktuell nicht auf 1 festgelegt oder nicht vorhanden ist, fügen Sie den Eintrag hinzu oder aktualisieren Sie den vorhandenen Eintrag entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routerankündigungen

Stellen Sie sicher, dass die VMware-Hostmaschinen die Annahme von Routerankündigungen und ICMP-Redirects verweigern, sofern nicht anderweitig für den Systembetrieb benötigt.

Mit IPv6 können Systeme ihre Netzwerkgeräte durch die automatische Verwendung von Informationen aus dem Netzwerk konfigurieren. Aus Sicherheitsgründen ist das manuelle Konfigurieren wichtiger Konfigurationsinformationen deren Annahme über das Netzwerk in einer nicht authentifizierten Art und Weise vorzuziehen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die Routerankündigungen verweigern.

Wenn die Hostmaschinen für die Verweigerung von IPv6 Routerankündigungen konfiguriert sind, gibt dieser Befehl Werte von 0 zurück:

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung von IPv6-Routerankündigungen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Wenn diese Einträge nicht vorhanden sind oder ihre Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routeranfragen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routeranfragen ablehnen, es sei denn, sie sind für den Systembetrieb erforderlich.

Die Einstellung der Routeranfragen bestimmt, wie viele Routeranfragen beim Anzeigen der Schnittstelle gesendet werden. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Anfragen zu senden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routeranfragen ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routeranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv6 Routereinstellungen bei Routeranfragen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routeranfragen ablehnen, es sei denn, sie sind für den Systembetrieb erforderlich.

Die Routereinstellungen in der Anfrageneinstellung bestimmen die Routereinstellungen. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Routereinstellungen für Anfragen zu empfangen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routeranfragen ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routeranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routerpräfixinformationen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routerpräfixinformationen verweigern, es sei denn, sie sind für den Systembetrieb erforderlich.

Die `accept_ra_pinfo`-Einstellung steuert, ob das System Präfixinformationen aus dem Router akzeptiert. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Routerpräfixinformationen zu empfangen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routerpräfixinformationen verweigern.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routerpräfixinformationen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der Hop-Limit-Einstellungen bei IPv6-Routerankündigungen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance Hop-Limit-Einstellungen der IPv6-Router verweigern, es sei denn, sie sind erforderlich.

Die `accept_ra_defrtr`-Einstellung steuert, ob das System Hop-Limit-Einstellungen aus einer Routerankündigung akzeptiert. Durch das Festlegen auf Null wird vorgebeugt, dass ein Router Ihr standardmäßiges IPv6-Hop-Limit für ausgehende Pakete ändert.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie Hop-Limit-Einstellungen der IPv6-Router verweigern.

Wenn die Hostmaschinen für die Verweigerung von Hop-Limit-Einstellungen der IPv6-Router konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der Hop-Limit-Einstellungen von IPv6- Routern konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern der Autoconf-Einstellungen von IPv6-Routerankündigungen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance Autoconf-Einstellungen der IPv6-Router verweigern, sofern nicht erforderlich.

Die `autoconf`-Einstellung steuert, ob Routerankündigungen das Zuweisen einer globalen Unicast-Adresse zu einer Schnittstelle durch das System verursachen können.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die Autoconf-Einstellungen der IPv6-Router verweigern.

Wenn die Hostmaschinen für die Verweigerung der Autoconf-Einstellungen von IPv6-Router konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der Autoconf-Einstellungen von IPv6-Router konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Nachbaranfragen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Nachbaranfragen verweigert, es sei denn, sie sind erforderlich.

Die `dad_transmits`-Einstellung legt fest, wie viele Nachbaranfragen pro Adresse (global und verbindungslokal) beim Anzeigen einer Schnittstelle gesendet werden, um sicherzustellen, dass die gewünschte Adresse im Netzwerk eindeutig ist.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie IPv6-Nachbaranfragen verweigern.

Wenn die Hostmaschinen für die Verweigerung von IPv6-Nachbaranfragen konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung von IPv6-Nachbaranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Einschränken der maximalen Anzahl der IPv6-Adressen

Stellen Sie sicher, dass die Einstellungen für die maximale Anzahl der IPv6-Adressen für die Hostmaschinen Ihrer VMware-Appliances auf eine für den Betrieb des Systems notwendige Mindestanzahl festgelegt sind.

Die Einstellung für die maximale Anzahl der Adressen legt fest, wie viele IPv6-Adressen auf jeder Schnittstelle zur Verfügung stehen. Der Standardwert lautet 16, aber Sie sollten genau die Anzahl der statisch konfigurierten globalen Adressen festlegen, die für Ihr System erforderlich ist.

Verfahren

- 1 Führen Sie den `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"`-Befehl auf den Hostmaschinen der VMware-Appliances aus, um sicherzustellen, dass die maximale Anzahl der IPv6-Adressen entsprechend eingeschränkt ist.

Wenn die Hostmaschinen zum Einschränken der maximalen Anzahl der IPv6-Adressen konfiguriert sind, gibt dieser Befehl die Werte 1 zurück.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie die maximale Anzahl der IPv6-Adressen auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Wenn die Einträge nicht vorhanden oder deren Werte nicht auf 1 gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Konfigurieren von Netzwerkeinstellungen für den Infrastructure as a Service-Host

Konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit die Einstellungen für die Netzwerkkommunikation auf der Hostmaschine der VMware-Infrastructure as a Service (IaaS)-Komponente gemäß den Anforderungen und Richtlinien von VMware.

Konfigurieren Sie die Netzwerkkonfiguration der Infrastructure as a Service (IaaS)-Hostmaschine, um die vollständigen vRealize Automation-Funktionen mit der entsprechenden Sicherheit zu unterstützen.

Siehe [Sichern der Infrastructure as a Service-Komponente](#).

Konfigurieren von Ports und Protokollen

Aus Sicherheitsgründen wird empfohlen, Ports und Protokolle für alle vRealize Automation-Appliances und -Komponenten gemäß den VMware-Richtlinien zu konfigurieren.

Konfigurieren Sie eingehende und ausgehende Ports für vRealize Automation-Komponenten gemäß den Anforderungen für kritische Systemkomponenten auf Produktionsebene. Deaktivieren Sie alle nicht benötigten Ports und Protokolle. Siehe [vRealize Automation-Referenzarchitektur](#).

Für Benutzer erforderliche Ports

Aus Sicherheitsgründen wird die Konfiguration der vRealize Automation-Benutzerports gemäß den VMware-Richtlinien empfohlen.

Legen Sie erforderliche Ports nur über ein sicheres Netzwerk offen.

SERVER	PORTS
vRealize Automation-Appliance	443, 8443

Für Administrator erforderliche Ports

Konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit vRealize Automation-Administratorports gemäß den VMware-Richtlinien.

Legen Sie erforderliche Ports nur über ein sicheres Netzwerk offen.

SERVER	PORTS
vRealize Application Services-Server	5480

vRealize Automation Appliance-Ports

Aus Sicherheitsgründen wird die Konfiguration von eingehenden und ausgehenden Ports für die vRealize Automation-Appliance gemäß den VMware-Empfehlungen empfohlen.

Eingehende Ports

Konfigurieren Sie die für die vRealize Automation-Appliance erforderliche Mindestanzahl an eingehenden Ports. Konfigurieren Sie optionale Ports, wenn diese für die Systemkonfiguration erforderlich sind.

Tabelle 1-4. Erforderliche Mindestanzahl an eingehenden Ports

PORT	PROTOKOLL	ANMERKUNGEN
443	TCP	Zugriff auf die vRealize Automation-Konsole und API-Aufrufe.
8443	TCP	Konsolen-Proxy (VMRC).
5480	TCP	Zugriff auf die Web-Verwaltungskonsole der virtuellen Appliance.
5488, 5489	TCP	Intern. Von der vRealize Automation-Appliance für Updates verwendet.

Tabelle 1-4. Erforderliche Mindestanzahl an eingehenden Ports (Fortsetzung)

PORT	PROTOKOLL	ANMERKUNGEN
5672	TCP	RabbitMQ-Messaging. Hinweis Wenn Sie vRealize Automation-Appliance-Instanzen clustern, müssen Sie möglicherweise die geöffneten Ports 4369 und 25672 konfigurieren.
40002	TCP	Für den vIDM-Dienst erforderlich. Beim Hinzufügen in einer HA-Konfiguration ist der gesamte externe Datenverkehr mit Ausnahme des Datenverkehrs von anderen vRealize Automation-Appliance-Knoten durch eine Firewall geschützt.

Konfigurieren Sie bei Bedarf optionale eingehende Ports.

Tabelle 1-5. Optionale eingehende Ports

PORT	PROTOKOLL	ANMERKUNGEN
22	TCP	(Optional) SSH. Deaktivieren Sie in einer Produktionsumgebung die SSH-Dienstüberwachung an Port 22 und schließen Sie Port 22.
80	TCP	(Optional) Umleitung an 443.

Ausgehende Ports

Konfigurieren Sie die erforderlichen ausgehenden Ports.

Tabelle 1-6. Erforderliche Mindestanzahl an ausgehenden Ports

PORT	PROTOKOLL	ANMERKUNGEN
25, 587	TCP, UDP	SMTP für das Senden von ausgehenden Benachrichtigungs-E-Mails.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
143, 993	TCP, UDP	IMAP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
443	TCP	Infrastructure as a Service-Manager Service über HTTPS.

Konfigurieren Sie bei Bedarf optionale ausgehende Ports.

Tabelle 1-7. Optionale ausgehende Ports

PORT	PROTOKOLL	ANMERKUNGEN
80	TCP	(Optional) Für das Abrufen von Softwareaktualisierungen. Sie können Aktualisierungen separat herunterladen und anwenden.
123	TCP, UDP	(Optional) Für das direkte Herstellen der Verbindung zu NTP anstatt der Verwendung von Hostzeit.

Infrastructure as a Service-Ports

Aus Sicherheitsgründen wird die Konfiguration der eingehenden und ausgehenden Ports für Infrastructure as a Service (IaaS)-Komponenten gemäß den VMware-Richtlinien empfohlen.

Eingehende Ports

Konfigurieren Sie die erforderliche Mindestanzahl an eingehenden Ports für die IaaS-Komponenten.

Tabelle 1-8. Erforderliche Mindestanzahl an eingehenden Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Manager Service	443	TCP	Kommunikation mit IaaS-Komponenten und vRealize Automation Appliance über HTTPS. Bei allen von Proxy-Agents verwalteten Virtualisierungshosts muss TCP-Port 443 für eingehenden Datenverkehr geöffnet sein.

Ausgehende Ports

Konfigurieren Sie die erforderliche Mindestanzahl an ausgehenden Ports für die IaaS-Komponenten.

Tabelle 1-9. Erforderliche Mindestanzahl an ausgehenden Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Alle	53	TCP, UDP	DNS.
Alle		TCP, UDP	DHCP.
Manager Service	443	TCP	Kommunikation mit vRealize Automation Appliance über HTTPS.
Website	443	TCP	Kommunikation mit Manager Service über HTTPS.
Distributed Execution Manager	443	TCP	Kommunikation mit Manager Service über HTTPS.
Proxy-Agents	443	TCP	Kommunikation mit Manager Service und Virtualisierungshosts über HTTPS.
Gast-Agent	443	TCP	Kommunikation mit Manager Service über HTTPS.
Manager Service, Website	1433	TCP	MSSQL.

Konfigurieren Sie optionale ausgehende Ports, falls erforderlich.

Tabelle 1-10. Optionale ausgehende Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Alle	123	TCP, UDP	NTP ist optional.

Überwachung und Protokollierung

Richten Sie als Best Practice im Hinblick auf die Sicherheit Überwachung und Protokollierung auf dem vRealize Automation-System gemäß den Empfehlungen für VMware ein.

Remoteprotokollierung auf einem zentralen Protokollhost bietet einen sicheren Speicher für Protokolldateien. Mit dem Erfassen von Protokolldateien auf einem zentralen Host können Sie die Umgebung mit einem einzigen Tool überwachen. Darüber hinaus können Sie eine Aggregatanalyse durchführen und nach Hinweisen auf Bedrohungen wie koordinierte Angriffe auf mehrere Entitäten innerhalb der Infrastruktur suchen. Die Protokollierung auf einem sicheren, zentralisierten Protokollserver kann das Verhindern von Protokollmanipulation unterstützen und bietet außerdem eine langfristige Prüfungsaufzeichnung.

Sicherstellen, dass der Remote-Protokollierungsserver sicher ist

Nachdem Angreifer die Sicherheit des Hostcomputers verletzt haben, versuchen diese oft, nach Protokolldateien zu suchen und diese zu manipulieren, um ihre Spuren zu verdecken und die Kontrolle zu behalten, ohne entdeckt zu werden. Durch das Sichern des Remote-Protokollierungsservers wird entsprechend die Verhinderung der Manipulation von Protokollen unterstützt.

Verwenden eines autorisierten NTP-Servers

Stellen Sie sicher, dass alle Hostmaschinen dieselbe relative Zeitquelle, einschließlich des relevanten Lokalisierungsoffsets, verwenden und dass Sie die relative Zeitquelle auf einen vereinbarten Zeitstandard wie z. B. die koordinierte Weltzeit (UTC) korrelieren können. Mit einem disziplinierten Herangehen an Zeitquellen können Sie schnell Aktionen eines Eindringlings nachverfolgen und korrelieren, wenn Sie die relevanten Protokolldateien überprüfen. Bei falschen Zeiteinstellungen kann es schwierig werden, Protokolldateien zur Erkennung von Angriffen zu untersuchen und zu korrelieren. Dies kann zu ungenauen Ergebnissen bei der Überprüfung führen.

Verwenden Sie mindestens drei NTP-Server von externen Zeitquellen oder konfigurieren Sie einige lokale NTP-Server auf einem vertrauenswürdigen Netzwerk, die wiederum deren Uhrzeit von mindestens drei externen Zeitquellen erhalten.

Installieren von vRealize Automation

Folgen Sie den Anweisungen zum Installieren einer neuen Instanz von vRealize Automation.

Überblick über die vRealize Automation -Installation

Sie können vRealize Automation zur Unterstützung von minimalen, Proof-of-Concept-Umgebungen oder in verschiedenen verteilten Unternehmenskonfigurationen installieren, die Produktions-Arbeitslasten verarbeiten können. Die Installation kann interaktiv sein oder im Hintergrund ausgeführt werden.

Nach der Installation beginnen Sie mit der Verwendung von vRealize Automation, indem Sie Ihr Setup anpassen und Mandanten konfigurieren, um Benutzern die Self-Service-Bereitstellung und Lebenszyklusverwaltung von Cloud-Diensten zu ermöglichen.

Informationen zur Installation von vRealize Automation

Je nach gewünschter Interaktivität gibt es verschiedene Möglichkeiten, vRealize Automation zu installieren.

Zur Installation stellen Sie eine vRealize Automation-Appliance bereit und schließen die Installation selbst mithilfe einer der folgenden Optionen ab:

- Konsolidierter, browserbasierter Installationsassistent
- Separate browserbasierte Appliance-Konfiguration und separate Windows-Installationen für IaaS-Serverkomponenten
- Befehlszeilenbasiertes automatisches Installationsprogramm, das Eingaben von einer Answer-Datei akzeptiert
- Installations-REST-API, die JSON-formatierte Eingaben akzeptiert

Sie können vRealize Automation auch mit vRealize Suite Lifecycle Manager installieren. Weitere Informationen finden Sie in der [vRealize Suite-Dokumentation](#).

Neu in dieser vRealize Automation -Installation

Wenn Sie frühere Versionen von vRealize Automation installiert haben, beachten Sie die Installationsänderungen in dieser Version, bevor Sie beginnen.

- Diese Version vereinfacht die Umbenennung der vRealize Automation-Appliance. Siehe [Ändern des Hostnamens der vRealize Automation-Appliance](#).
- In dieser Version verwendet die vRealize Automation-Appliance standardmäßig TLS 1.2. Für das Update vorhandener Agents auf diese Version umfasst die Verwaltungsschnittstelle eine Option zur vorübergehenden Aktivierung von TLS 1.0 und 1.1.
- Die Verwaltungsschnittstelle der vRealize Automation-Appliance enthält jetzt eine Seite für die Installation und Verwaltung von Patches. Siehe [Zugriff auf Patch-Verwaltung](#).
- In dieser Version wird beschrieben, wie der Standard-Proxy-Port für VMware Remote Console geändert wird. Siehe [Ändern des VMware Remote Console-Proxy-Ports](#).
- In dieser Version werden einige fehlerhafte Hilfe-Links im Installationsassistenten korrigiert.

vRealize Automation -Installationskomponenten

Eine typische vRealize Automation-Installation besteht aus einer vRealize Automation-Appliance und einem oder mehreren Windows-Servern, die vRealize Automation als Infrastructure as a Service (IaaS) bereitstellen.

Die vRealize Automation -Appliance

Die vRealize Automation-Appliance ist eine vorkonfigurierte virtuelle Linux-Appliance. Die vRealize Automation-Appliance wird als offene Virtualisierungsdatei geliefert, die Sie auf einer vorhandenen virtualisierten Infrastruktur wie vSphere bereitstellen.

Die vRealize Automation-Appliance führt mehrere Funktionen aus, die für vRealize Automation wichtig sind.

- Die Appliance enthält den Server, der das vRealize Automation-Produktportal hostet, auf dem Benutzer für die Self-Service-Bereitstellung und Verwaltung von Cloud-Diensten anmelden.

- Die Appliance verwaltet Single Sign-On (SSO) für die Benutzerautorisierung und -authentifizierung.
- Der Appliance-Server hostet eine Verwaltungsschnittstelle für die Einstellungen der vRealize Automation-Appliance.
- Die Appliance enthält eine vorkonfigurierte PostgreSQL-Datenbank für interne Vorgänge der vRealize Automation-Appliance.

In großen Bereitstellungen mit redundanten Appliances dienen die sekundären Appliance-Datenbanken als Replikate, um Hochverfügbarkeit bieten zu können.

- Die Appliance enthält eine vorkonfigurierte Instanz von vRealize Orchestrator. Zur Erweiterung seiner Kapazitäten verwendet vRealize Automation vRealize Orchestrator-Workflows und Aktionen.

Es empfiehlt sich die eingebettete Instanz von vRealize Orchestrator-. Bei älteren Bereitstellungen oder für Spezialfälle können Benutzer jedoch vRealize Automation mit einer externen vRealize Orchestrator-Instanz verbinden.

- Die Appliance enthält das herunterladbare Installationsprogramm des Management-Agents. Alle Windows-Server, aus denen Ihr vRealize AutomationIaaS besteht, müssen den Management-Agent installieren.

Der Management-Agent registriert die IaaS-Windows-Server bei der vRealize Automation-Appliance, automatisiert die Installation und Verwaltung von IaaS-Komponenten und erfasst Support- und Telemetriedaten.

Infrastructure as a Service

vRealize Automation IaaS besteht aus einem oder mehreren Windows-Servern, die zur Modellierung und Bereitstellung von Systemen in privaten, öffentlichen oder hybriden Cloud-Infrastrukturen zusammenarbeiten.

Sie installieren vRealize Automation-Komponenten von IaaS auf einem oder mehreren virtuellen oder physischen Windows-Servern. Nach der Installation erscheinen IaaS-Vorgänge auf der Registerkarte „Infrastruktur“ in der Produktschnittstelle.

IaaS besteht aus folgenden Komponenten, die je nach Bereitstellungsgröße gemeinsam oder einzeln installiert werden können.

Webserver

Der IaaS-Webserver bietet Infrastrukturverwaltung und -Dienste für die vRealize Automation-Produktschnittstelle. Die Webserver-Komponente kommuniziert mit dem Manager Service, der die Updates vom Distributed Execution Manager (DEM), der SQL Server-Datenbank und den Agents zur Verfügung stellt.

Model Manager

vRealize Automation-Modelle vereinfachen die Integration in externe Systeme und Datenbanken. Sie implementieren Geschäftslogik, die vom DEM verwendet wird.

Der Model Manager stellt Dienste und Dienstprogramme für Persistenz, Versionierung, Sichern und Verteilen von Modellelementen bereit. Der Model Manager wird auf einem der IaaS-Webserver gehostet und kommuniziert mit DEMs, der SQL Server-Datenbank und der Produktschnittstellen-Website.

Manager Service

Der Manager Service ist ein Windows-Dienst, der die Kommunikation zwischen IaaS-DEMs, der SQL Server-Datenbank, den Agents und SMTP koordiniert. Der Manager-Dienst kommuniziert zudem mit dem Webserver über den Model Manager und muss unter einem Domänenkonto mit lokalen Administratorrechten auf allen IaaS-Windows-Servern ausgeführt werden.

Wenn Sie automatisches Manager Service-Failover aktivieren, verlangt IaaS, dass der Manager-Dienst nicht auf mehreren, sondern nur auf einer aktiven Windows-Maschine ausgeführt wird. Für Sicherungen oder Hochverfügbarkeit können Sie zusätzliche Manager-Dienst-Maschinen bereitstellen. Das Konzept des manuellen Failovers setzt jedoch voraus, dass der Dienst auf Sicherungsmaschinen beendet und für den manuellen Start konfiguriert ist.

Weitere Informationen finden Sie unter [Informationen zum automatischen Manager Service-Failover](#).

SQL Server-Datenbank

IaaS verwendet eine Microsoft SQL Server-Datenbank, um Informationen zu den verwalteten Maschinen und zu den eigenen Elementen und Richtlinien zu warten. Die meisten Benutzer erlauben vRealize Automation eine Erstellung der Datenbank während der Installation. Alternativ dazu können Sie die Datenbank separat gemäß Ihren Standortrichtlinien erstellen.

Distributed Execution Manager

Die IaaS-DEM-Komponente führt die Geschäftslogik von benutzerdefinierten Modellen aus, die mit der IaaS SQL Server-Datenbank und mit externen Datenbanken und Systemen interagiert. Üblicherweise werden DEMs auf dem IaaS-Windows-Server installiert, der den aktiven Manager Service hostet. Diese Vorgehensweise ist jedoch nicht zwingend erforderlich.

Jede DEM-Instanz kann die Rolle eines Workers oder eines Orchestrators übernehmen. Die Rollen können auf demselben oder auf separaten Servern installiert werden.

DEM-Worker – Ein DEM-Worker hat eine Funktion: die Ausführung des Workflows. Mehrere DEM-Worker erweitern die Kapazität und können auf demselben oder auf separaten Servern installiert werden.

DEM-Orchestrator – Ein DEM-Orchestrator führt folgende Überwachungsfunktionen aus.

- Überwacht DEM-Worker. Wenn ein Worker die Arbeit einstellt oder seine Verbindung zum Model Manager verliert, leitet der DEM-Orchestrator die Workflows zu einem anderen DEM-Worker.
- Plant Workflows durch das Erstellen neuer Workflowinstanzen zum geplanten Zeitpunkt.
- Stellt sicher, dass jeweils nur eine Instanz eines geplanten Workflows ausgeführt wird.
- Führt eine Vorverarbeitung der Workflows vor der Ausführung durch. Bei der Vorverarbeitung werden die Voraussetzungen für Workflows überprüft und der Ausführungsverlauf für den jeweiligen Workflow erstellt.

Der aktive DEM-Orchestrator benötigt eine gute Netzwerkverbindung zum Model Manager-Host. In großen Bereitstellungen mit mehreren DEM-Orchestratoren auf separaten Servern dienen die sekundären Orchestratoren als Sicherungen. Die sekundären DEM-Orchestratoren überwachen den aktiven DEM-Orchestrator und bieten Redundanz und Failover, wenn ein Problem mit den aktiven DEM-Orchestrator auftritt. Bei dieser Art der Failover-Konfiguration könnte sich eine Installation des aktiven DEM-Orchestrators mit dem aktiven Manager Service-Host sowie der sekundären DEM-Orchestratoren mit den betriebsbereiten Manager Service-Hosts als sinnvoll erweisen.

Agents

vRealize Automation IaaS verwendet Agents für die Integration in externe Systeme und für die Verwaltung von Informationen in vRealize Automation-Komponenten.

Üblicherweise werden vRealize Automation-Agents auf dem IaaS-Windows-Server installiert, der den aktiven Manager Service hostet. Diese Vorgehensweise ist jedoch nicht zwingend erforderlich. Mehrere Agents erweitern die Kapazität und können auf demselben oder auf separaten Servern installiert werden.

Virtualisierungs-Proxy-Agents

vRealize Automation erstellt und verwaltet virtuelle Maschinen auf Virtualisierungshosts. Virtualisierungs-Proxy-Agents senden Befehle und erfassen Daten von vSphere ESX Server, XenServer und Hyper-V-Hosts und den auf diesen bereitgestellten virtuellen Maschinen.

Ein Virtualisierungs-Proxy-Agent weist die folgenden Merkmale auf.

- Erfordert üblicherweise Administratorrechte auf der von ihm verwalteten Virtualisierungsplattform.
- Kommuniziert mit dem IaaS-Manager Service.
- Wird separat mit einer eigenen Konfigurationsdatei installiert.

Die meisten vRealize Automation-Bereitstellungen installieren den vSphere-Proxy-Agent. Je nach Virtualisierungsressourcen an Ihrem Standort können Sie andere Proxy-Agents installieren.

Virtual Desktop Integration-Agents

Virtual Desktop Integration (VDI) PowerShell-Agents ermöglichen vRealize Automation die Integration in externe virtuelle Desktopsysteme. VDI-Agents benötigen Administratorrechte auf den externen Systemen.

Sie können virtuelle Maschinen registrieren, die von vRealize Automation mit XenDesktop auf einem Citrix Desktop Delivery Controller (DDC) bereitgestellt werden, sodass Benutzer auf die XenDesktop-Webchnittstelle von vRealize Automation zugreifen können.

External Provisioning Integration-Agents

External Provisioning Integration (EPI) PowerShell-Agents ermöglichen vRealize Automation die Integration externer Systeme in den Maschinenbereitstellungsprozess.

Beispielsweise ermöglicht die Integration in den Citrix Provisioning Server die Bereitstellung von Maschinen per bedarfsgesteuertem Festplatten-Streaming, und ein EPI-Agent ermöglicht die Ausführung von Visual Basic-Skripts als zusätzliche Schritte während des Bereitstellungsprozesses.

EPI-Agents benötigen Administratorrechte auf den externen Systemen, mit denen sie interagieren.

Windows-Verwaltungsinstrumentations-Agent (WMI)

Der vRealize Automation Windows-Verwaltungsinstrumentations-Agent (WMI) optimiert die Überwachung und Kontrolle der Windows-Systeminformationen und ermöglicht die zentrale Verwaltung von Windows-Remote-Servern. Darüber hinaus bietet der WMI-Agent auch die Sammlung von Daten von Windows-Servern, die von vRealize Automation verwaltet werden.

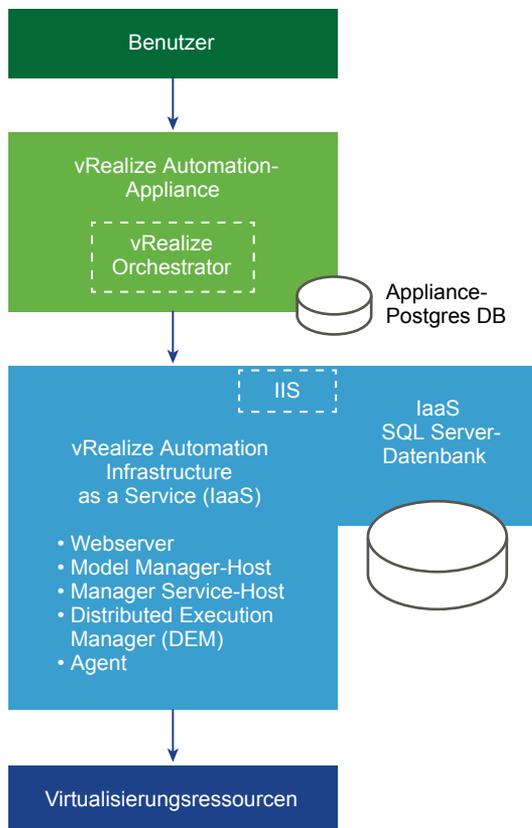
Bereitstellungstyp

Sie können vRealize Automation als Mindestbereitstellung zu Proof-of-Concept-Zwecken oder für Entwicklungsarbeiten oder als verteilte Konfiguration für mittlere bis große Produktionsarbeitslasten installieren.

Minimalbereitstellungen von vRealize Automation

Minimalbereitstellungen enthalten eine vRealize Automation-Appliance und einen Windows-Server, der die IaaS-Komponenten hostet. In einer Minimalbereitstellung kann sich die SQL Server-Datenbank von vRealize Automation auf demselben IaaS-Windows-Server mit den IaaS-Komponenten oder auf einem separaten Windows-Server befinden.

Abbildung 1-10. Minimalbereitstellung von vRealize Automation



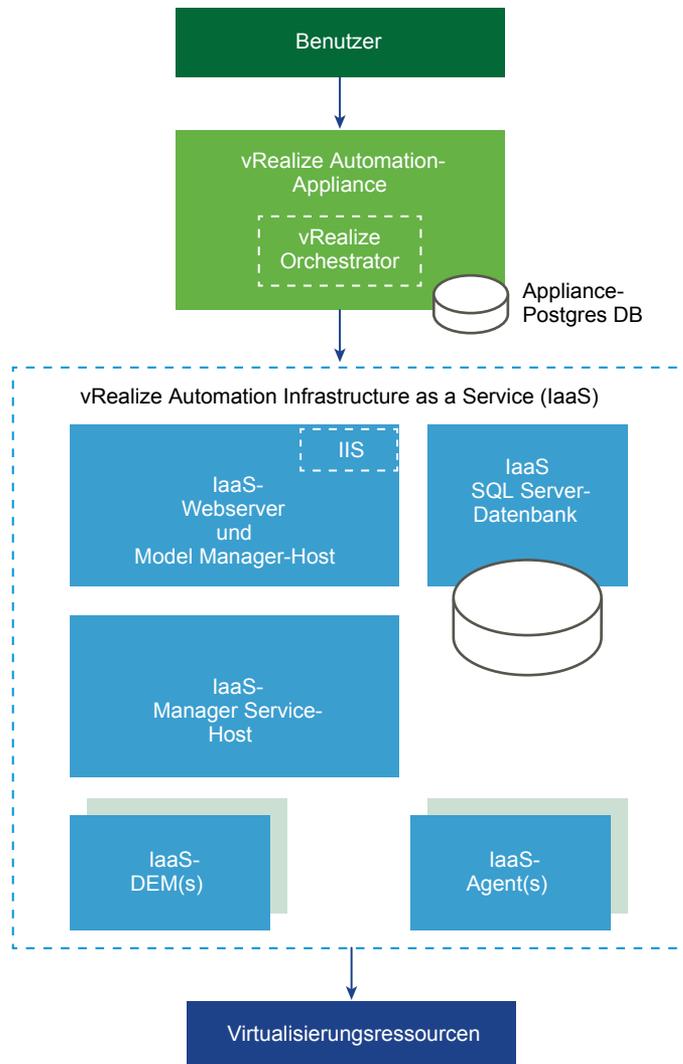
Eine Minimalbereitstellung kann nicht in eine Unternehmensbereitstellung konvertiert werden. Beginnen Sie zum Hochskalieren einer Bereitstellung mit einer kleinen Unternehmensbereitstellung und fügen Sie darin Komponenten hinzu. Eine Minimalbereitstellung wird als Ausgangspunkt nicht unterstützt.

Hinweis Die vRealize Automation-Dokumentation enthält eine komplette Beispiel-Minimalbereitstellung, die Sie durch die Installation führt und Ihnen zeigt, wie Sie das Produkt für Proof-of-Concept-Zwecke verwenden können. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.

Verteilte Bereitstellungen von vRealize Automation

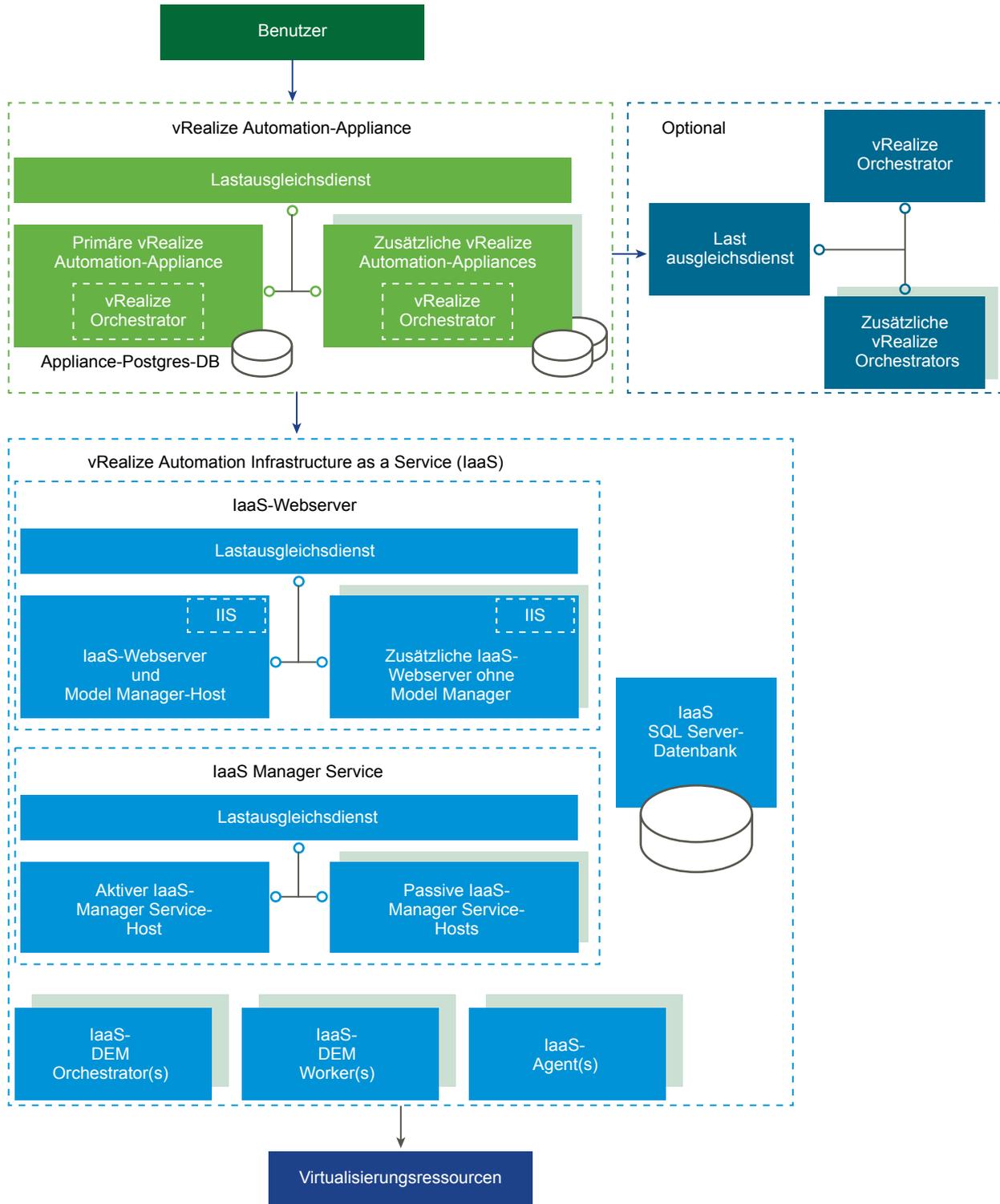
Verteilte Unternehmensbereitstellungen können verschiedene Größen haben. Eine einfache verteilte Bereitstellung kann vRealize Automation verbessern, indem IaaS-Komponenten auf separaten Windows-Servern gehostet werden (siehe folgende Abbildung).

Abbildung 1-11. Verteilte Bereitstellung von vRealize Automation



Viele Produktionsbereitstellungen gehen mit redundanten Appliances, redundanten Servern und sogar Lastausgleichsdiensten für noch mehr Kapazität noch weiter. Große, verteilte Bereitstellungen bieten bessere Skalierung, Hochverfügbarkeit und Notfallwiederherstellung. Bitte beachten Sie, dass wir jetzt die eingebettete Instanz von vRealize Orchestrator empfehlen. Möglicherweise ist vRealize Automation aber auch mit einem externen vRealize Orchestrator in älteren Bereitstellungen verbunden.

Abbildung 1-12. Große verteilte und mit Lastausgleichsdienst arbeitende vRealize Automation -Bereitstellung



Informationen zur Skalierbarkeit und Hochverfügbarkeit finden Sie im Handbuch *vRealize Automation Referenzarchitektur*.

Auswählen der Installationsmethode

Der konsolidierte Installationsassistent von vRealize Automation ist Ihr primäres Tool für neue vRealize Automation-Installationen. Alternativ können Sie die manuellen, separaten Installationsvorgänge oder eine automatische Installation durchführen.

- Mit dem Installationsassistenten können Sie schnell und einfach installieren, ganz egal, ob es sich um kleine oder verteilte Bereitstellungen für Unternehmen mit oder ohne Lastausgleichsdienst handelt. Die meisten Benutzer führen den Installationsassistenten aus.
- Wenn Sie eine vRealize Automation-Bereitstellung erweitern möchten oder wenn der Installationsassistent aus einem beliebigen Grund beendet wurde, benötigen Sie die manuellen Installationsschritte. Nachdem Sie eine manuelle Installation gestartet haben, können Sie nicht mehr zum Installationsassistenten zurückkehren.
- Je nach den Anforderungen Ihrer Site können Sie auch eine automatische Installation, eine Befehlszeileninstallation oder eine API-basierte Installation durchführen.

Vorbereitung für die Installation von vRealize Automation

Sie installieren vRealize Automation in einer vorhandenen Virtualisierungsinfrastruktur. Bevor Sie mit einer Installation beginnen, müssen Sie bestimmte umgebungsabhängige Anforderungen sowie Systemanforderungen erfüllen.

Allgemeine Vorbereitung

Vor der Installation von vRealize Automation sollten Sie einige Punkte für die gesamte Bereitstellung beachten.

Weitere Informationen zu den allgemeinen Umgebungsanforderungen, einschließlich unterstützte Betriebssysteme und Browserversionen, finden Sie in der [vRealize Automation-Support-Matrix](#).

Webbrowser für Benutzer

Mehrere Browserfenster und -registerkarten werden nicht unterstützt. vRealize Automation unterstützt eine Sitzung pro Benutzer.

In vSphere bereitgestellte VMware-Remote-Konsolen unterstützen einen Teil der von vRealize Automation unterstützten Browser.

Drittanbieter-Software

Drittanbieter-Software sollte mit den neuesten Anbieter-Patches ausgestattet sein. Drittanbieter-Software beinhaltet Microsoft Windows und SQL Server.

Uhrzeitsynchronisierung

Alle vRealize Automation-Appliances und IaaS Windows-Server müssen mit derselben Uhrzeitquelle synchronisiert werden. Möglicherweise können Sie nur eine der folgenden Quellen verwenden. Vermischen Sie die Zeitquellen nicht.

- Der vRealize Automation-Appliance-Host
- Ein externer NTP-Server

Um den vRealize Automation-Appliance-Host zu verwenden, müssen Sie NTP auf dem ESXi-Host ausführen. Weitere Informationen zur Zeiterfassung finden Sie im [VMware-Knowledgebase-Artikel 1318](#).

Sie wählen die Zeitquelle auf der Seite „Installationsvoraussetzungen“ des Installationsassistenten aus.

Konten und Kennwörter

Es gibt mehrere Benutzerkonten und Kennwörter, die Sie möglicherweise zum Erstellen oder Planen der Einstellungen vor der Installation von vRealize Automation benötigen.

IaaS -Dienstkonto

IaaS installiert mehrere Windows-Dienste, die unter einem einzelnen Benutzerkonto ausgeführt werden müssen.

- Das Konto muss ein Domänenbenutzer sein.
- Das Konto muss kein Domänenadministrator sein, muss aber vor der Installation auf allen IaaS Windows-Servern über lokale Administratorrechte verfügen.
- Das Kennwort für das Konto darf keine doppelten Anführungszeichen (") enthalten.
- Sie werden vom Management-Agent-Installationsprogramm für IaaS Windows-Server zur Eingabe der Anmeldedaten aufgefordert.
- Das Konto muss über die Berechtigung **Als Dienst anmelden** verfügen, damit der Manager-Dienst gestartet und die Protokolldateien generiert werden können.
- Das Konto muss die „db_owner“-Berechtigung für die IaaS-Datenbank aufweisen.

Wenn Sie das Installationsprogramm zum Erstellen der Datenbank verwenden, fügen Sie vor der Installation die Kontoanmeldung zum SQL Server hinzu. Das Installationsprogramm gewährt die „db_owner“-Berechtigung nach dem Erstellen der Datenbank.

- Wenn Sie das Installationsprogramm zum Erstellen der Datenbank verwenden, fügen Sie dem Konto in der SQL-Instanz vor der Installation die Rolle „sysadmin“ hinzu.

Die Rolle „sysadmin“ ist nicht erforderlich, wenn Sie eine vorhandene leere Datenbank verwenden.

Identität des IIS-Anwendungspools

Das Konto, das Sie als Identität des IIS-Anwendungspools für den Model Manager-Webdienst verwenden, muss über die Berechtigung **Anmelden als Stapelverarbeitungsauftrag** verfügen.

IaaS -Datenbankanmeldedaten

Sie können die Datenbank entweder über das vRealize Automation-Installationsprogramm oder separat mithilfe von SQL Server erstellen. Wenn das vRealize Automation-Installationsprogramm die Datenbank erstellt, gelten die folgenden Anforderungen.

- Wenn Sie für das vRealize Automation-Installationsprogramm die Windows-Authentifizierung auswählen, muss das Konto, das den Management-Agent auf dem primären IaaS-Webserver ausführt, über die Rolle „sysadmin“ in der SQL-Instanz verfügen, um die Größe der Datenbank festzulegen und zu ändern.
- Auch wenn Sie für das vRealize Automation-Installationsprogramm die Windows-Authentifizierung nicht auswählen, muss das Konto, das den Management-Agent auf dem primären IaaS-Webserver ausführt, über die Rolle „sysadmin“ in der SQL-Instanz verfügen, da die Anmeldedaten zur Laufzeit verwendet werden.
- Wenn Sie die Datenbank separat erstellen, sind für die von Ihnen angegebenen Windows- oder SQL-Benutzeranmeldedaten lediglich „db_owner“-Berechtigungen für die Datenbank erforderlich.

Passphrase für die IaaS -Datenbanksicherheit

Die Passphrase für die Datenbanksicherheit generiert einen Verschlüsselungsschlüssel, der die Daten in der IaaS SQL-Datenbank schützt. Sie geben die Sicherheits-Passphrase auf der Seite „IaaS-Host“ im Installationsassistenten an.

- Verwenden Sie dieselbe Passphrase für die Datenbanksicherheit für die gesamte Installation, sodass jede Komponente denselben Verschlüsselungsschlüssel hat.
- Notieren Sie die Passphrase, da Sie sie zum Wiederherstellen der Datenbank benötigen, wenn ein Failover eintritt oder Sie nach der Erstinstallation Komponenten hinzufügen.
- Die Passphrase für die Datenbanksicherheit darf kein doppeltes Anführungszeichen (") enthalten. Die Passphrase wird akzeptiert, wenn Sie sie erstellen, die Installation schlägt jedoch fehl.

vSphere -Endpoints

Wenn Sie einen vSphere-Endpoint bereitstellen möchten, benötigen Sie eine Domäne oder ein lokales Konto mit ausreichend Berechtigungen zum Ausführen von zweiseitigen Vorgängen. Für das Konto muss ebenfalls die entsprechende Berechtigungsebene in vRealize Orchestrator konfiguriert werden.

vRealize Automation -Administratorkennwort

Nach der Installation können Sie sich mit dem vRealize Automation-Administratorkennwort beim Standardmandanten anmelden. Sie geben das Administratorkennwort auf der Single Sign-On-Seite des Installationsassistenten an.

Das vRealize Automation-Administratorkennwort darf kein angehängtes Gleichheitszeichen (=) enthalten. Das Kennwort wird akzeptiert, während Sie es erstellen. Wenn Sie jedoch zu einem späteren Zeitpunkt Aktionen durchführen, wie zum Beispiel Endpoints speichern, treten Fehler auf.

Hostnamen und IP-Adressen

vRealize Automation verlangt, dass bei der Benennung von Hostnamen in Ihrer Installation bestimmte Voraussetzungen erfüllt sein müssen.

- Alle vRealize Automation-Maschinen in Ihrer Installation müssen sich gegenseitig über den vollqualifizierten Domännennamen (FQDN) auflösen können.

Geben Sie bei der Installation stets den vollqualifizierten Domännennamen (FQDN) ein, wenn Sie eine vRealize Automation-Maschine angeben oder auswählen. Geben Sie keine IP-Adressen oder kurzen Computernamen ein.

- Neben der Anforderung hinsichtlich des FQDN müssen sich Windows-Maschinen, die den Model Manager Web-Dienst, den Manager Service und die Microsoft SQL Server-Datenbank hosten, gegenseitig über den WINS-Namen (Windows Internet Name Service) auflösen können.

Konfigurieren Sie DNS (Domain Name System) für die Auflösung dieser kurzen WINS-Hostnamen.

- Planen Sie die Benennung von Domänen und Maschinen im Voraus, sodass die Namen von vRealize Automation-Maschinen mit Buchstaben (a–z, A–Z) beginnen, mit Buchstaben oder Ziffern (0–9) enden und dazwischen nur Buchstaben, Ziffern oder Bindestriche (-) enthalten. Unterstriche (_) sind im Hostnamen oder an beliebiger Stelle im FQDN nicht zulässig.

Weitere Informationen zu zulässigen Namen erhalten Sie in den Spezifikationen für Hostnamen und von der Internet Engineering Task Force unter www.ietf.org.

- Behalten Sie die für vRealize Automation-Systeme geplanten Hostnamen und FQDNs möglichst bei. Ein Hostname kann nicht immer geändert werden. Wenn eine Änderung möglich ist, kann dies ein komplizierter Vorgang sein.
- Es empfiehlt sich, statische IP-Adressen für alle vRealize Automation-Appliances und IaaS-Windows-Server zu reservieren und zu verwenden. vRealize Automation unterstützt zwar DHCP, für langfristige Bereitstellungen wie Produktionsumgebungen werden jedoch statische IP-Adressen empfohlen.
 - IP-Adressen werden der vRealize Automation-Appliance bei der OVF- oder OVA-Bereitstellung zugewiesen.
 - Führen Sie für die IaaS-Windows-Server die üblichen Vorgänge für Betriebssysteme durch. Legen Sie die IP-Adresse vor der Installation von vRealize Automation IaaS fest.

Latenz und Bandbreite

vRealize Automation unterstützt die verteilte Installation auf mehreren Sites, aber die Datenübertragungsraten und das Volumen müssen minimale Voraussetzungen erfüllen.

vRealize Automation benötigt eine Umgebung mit einer Netzwerklatenz von höchstens 5 ms und einer Bandbreite von mindestens 1 GB zwischen den folgenden Komponenten.

- vRealize Automation-Appliance
- IaaS-Webserver
- IaaS Model Manager-Host

- IaaS Manager Service-Host
- IaaS SQL Server-Datenbank
- IaaS DEM Orchestrator

Die folgende Komponente funktioniert möglicherweise auf einer Site mit höherer Latenz, die Vorgehensweise wird allerdings nicht empfohlen.

- IaaS DEM Worker

Sie können die folgende Komponente auf der Site des Endpoints installieren, mit dem sie kommuniziert.

- IaaS Proxy-Agent

vRealize Automation -Appliance

Die meisten Anforderungen an die vRealize Automation-Appliance sind in der von Ihnen bereitgestellten OVF oder OVA vorkonfiguriert. Für eigenständige, Master- oder vRealize Automation Replikat-Appliances gelten die gleichen Anforderungen.

Die Mindesthardware der virtuellen Maschine, auf der Sie die Bereitstellung durchführen können, ist Version 7 oder ESX/ESXi 4.x oder höher. Siehe [VMware-Knowledgebase-Artikel 2007240](#). Führen Sie die Bereitstellung aufgrund des Bedarfs an Hardwareressourcen nicht unter VMware Workstation durch.

Nach der Bereitstellung können Sie mithilfe von vSphere die Hardwareeinstellungen der vRealize Automation-Appliance anpassen, um die Active Directory-Anforderungen zu erfüllen. Weitere Informationen finden Sie in der folgenden Tabelle.

Tabelle 1-11. Hardwareanforderungen an die vRealize Automation -Appliance für Active Directory

vRealize Automation-Appliance für kleine Active Directories	vRealize Automation-Appliance für große Active Directories
<ul style="list-style-type: none"> ■ 4 CPUs ■ 18 GB Arbeitsspeicher ■ 60 GB Festplattenspeicher 	<ul style="list-style-type: none"> ■ 4 CPUs ■ 22 GB Arbeitsspeicher ■ 60 GB Festplattenspeicher

Ein kleines Active Directory verfügt über 25.000 Benutzer in der Organisationseinheit (OU), die in der ID-Speicherkonfiguration synchronisiert werden. Ein großes Active Directory verfügt über mehr als 25.000 Benutzer in der Organisationseinheit.

vRealize Automation Appliance-Ports

Die Ports der vRealize Automation-Appliance sind in der von Ihnen bereitgestellten OVF oder OVA üblicherweise vorkonfiguriert.

Die folgenden Ports werden von der vRealize Automation-Appliance verwendet.

Tabelle 1-12. Eingehende Ports

Port	Protokoll	Anmerkungen
22	TCP	Optional. Zugriff auf SSH-Sitzungen.
80	TCP	Optional. Leitet weiter zu 443.

Tabelle 1-12. Eingehende Ports (Fortsetzung)

Port	Protokoll	Anmerkungen
88	TCP (UDP optional)	Cloud KDC-Kerberos-Authentifizierung von externen mobilen Geräten.
443	TCP	Zugriff auf die vRealize Automation-Konsole und API-Aufrufe. Zugriff für Maschinen zum Herunterladen des Gast-Agents und des Software-Bootstrap-Agents. Zugriff für Lastausgleichsdienst, Browser.
4369, 5671, 5672, 25672	TCP	RabbitMQ-Messaging.
5480	TCP	Zugriff auf die Verwaltungsschnittstelle der virtuellen Appliance. Verwendet vom Management-Agent.
5488, 5489	TCP	Intern von der vRealize Automation-Appliance für Updates verwendet.
8230, 8280, 8281, 8283	TCP	Interne vRealize Orchestrator-Instanz.
8443	TCP	Zugriff für Browser. Administratorport für Identity Manager über HTTPS.
8444	TCP	Konsolenproxykommunikation für vSphere VMware Remote Console-Verbindungen.
9300–9400	TCP	Zugriff für Identity Manager-Audits.
54328	UDP	

Tabelle 1-13. Ausgehende Ports

Port	Protokoll	Anmerkungen
25, 587	TCP, UDP	SMTP für das Senden von ausgehenden Benachrichtigungs-E-Mails.
53	TCP, UDP	DNS-Server.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Optional. Für das Abrufen von Softwareaktualisierungen. Aktualisierungen können separat heruntergeladen und angewendet werden.
88, 464, 135	TCP, UDP	Domänencontroller.
110, 995	TCP, UDP	POP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
143, 993	TCP, UDP	IMAP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
123	TCP, UDP	Optional. Für das direkte Herstellen der Verbindung zu NTP anstatt der Verwendung von Hostzeit.
389	TCP	Zugriff auf View-Verbindungsserver.
389, 636, 3268, 3269	TCP	Active Directory. Standardports angezeigt, sind aber konfigurierbar.
443	TCP	Kommunikation mit IaaS Manager Service und Infrastruktur-Endpoint-Hosts über HTTPS Kommunikation mit dem vRealize Automation-Softwaredienst über HTTPS. Zugriff auf den Identity Manager-Upgrade-Server.

Tabelle 1-13. Ausgehende Ports (Fortsetzung)

Port	Protokoll	Anmerkungen
		Zugriff auf View-Verbindungsserver.
445	TCP	Zugriff auf ThinApp-Repository für Identity Manager.
902	TCP	Kopiervorgänge für ESXi-Netzwerkdatei und VMware Remote Console-Verbindungen.
5050	TCP	Optional. Für die Kommunikation mit vRealize Business for Cloud.
5432	TCP, UDP	Optional. Für die Kommunikation mit der PostgreSQL-Datenbank einer anderen Appliance.
5500	TCP	RSA SecurID-System. Standardport angezeigt, ist aber konfigurierbar.
8281	TCP	Optional. Für die Kommunikation mit einer externen vRealize Orchestrator-Instanz.
9300–9400	TCP	Zugriff für Identity Manager-Audits.
54328	UDP	

Andere Ports sind möglicherweise durch bestimmte vRealize Orchestrator-Plug-Ins erforderlich, die mit externen Systemen kommunizieren. Informieren Sie sich in der Dokumentation für das vRealize Orchestrator-Plug-In.

IaaS -Windows-Server

Alle Windows-Server, die IaaS-Komponenten hosten, müssen bestimmte Anforderungen erfüllen. Sorgen Sie dafür, dass die Anforderungen erfüllt sind, bevor Sie den Installationsassistenten für vRealize Automation oder das Standardinstallationsprogramm von Windows ausführen.

- Platzieren Sie alle IaaS-Windows-Server in derselben Domäne. Verwenden Sie keine Arbeitsgruppen.
- Jeder Server benötigt die folgende Mindesthardware.
 - 2 CPUs
 - 8 GB Arbeitsspeicher
 - 40 GB Festplattenspeicher

Ein Server, der die SQL-Datenbank zusammen mit IaaS-Komponenten hostet, benötigt eventuell zusätzliche Hardware.

- Führen Sie die Bereitstellung aufgrund des Bedarfs an Hardwareressourcen nicht unter VMware Workstation durch.
- Installieren Sie Microsoft .NET Framework 3.5.
- Installieren Sie Microsoft .NET Framework 4.5.2 oder höher.

Eine Kopie von .NET ist über jede vRealize Automation-Appliance verfügbar:

<https://vrealize-automation-appliance-fqdn:5480/installer/>

Achten Sie bei Verwendung von Internet Explorer zum Herunterladen darauf, dass „Verstärkte Sicherheitskonfiguration“ deaktiviert ist. Navigieren Sie auf dem Windows-Server zu „res://iesetup.dll/SoftAdmin.htm“.

- Installieren Sie je nach Ihrer Windows-Version Microsoft PowerShell 2.0, 3.0 oder 4.0.

Beachten Sie, dass Sie für manche vRealize Automation-Upgrades oder -Migrationen zusätzlich zur aktuell verwendeten PowerShell-Version möglicherweise eine ältere oder neuere PowerShell-Version installieren müssen.

- Wenn Sie mehr als eine IaaS-Komponente auf demselben Windows-Server installieren, sollten Sie diese im selben Installationsordner installieren. Verwenden Sie keine unterschiedlichen Pfade.
- IaaS-Server verwenden TLS zur Authentifizierung; dies ist standardmäßig auf einigen Windows-Servern aktiviert.

Einige Sites deaktivieren TLS aus Sicherheitsgründen, aber Sie müssen mindestens ein TLS-Protokoll aktiviert lassen. Diese Version von vRealize Automation unterstützt TLS 1.2.

- Aktivieren Sie den DTC-Dienst (Distributed Transaction Coordinator). IaaS verwendet DTC für Datenbanktransaktionen und Aktionen wie beispielsweise die Erstellung von Workflows.

Hinweis Wenn Sie eine Maschine klonen, um einen IaaS-Windows-Server zu erstellen, installieren Sie DTC nach dem Klonvorgang auf dem Klon. Wenn Sie eine Maschine klonen, für die DTC bereits installiert ist, wird ihr eindeutiger Bezeichner auf den Klon kopiert, wodurch die Kommunikation fehlschlägt. Siehe [Fehler bei der Kommunikation mit dem Manager Service](#).

Aktivieren Sie DTC auch auf dem Server, der die SQL-Datenbank hostet, falls dieser von IaaS getrennt ist. Weitere Informationen zur DTC-Aktivierung finden Sie im [VMware-Knowledgebase-Artikel 2038943](#).

- Stellen Sie sicher, dass der sekundäre Anmeldedienst ausgeführt wird. Falls gewünscht, können Sie den Dienst nach Abschluss der Installation beenden.

Ports auf IaaS -Windows-Servern

Ports auf IaaS-Windows-Servern müssen vor der Installation von vRealize Automation konfiguriert werden.

Öffnen Sie die Ports zwischen allen IaaS Windows-Servern gemäß den folgenden Tabellen. Schließen Sie den Server ein, der die SQL-Datenbank hostet, wenn diese von IaaS getrennt ist. Alternativ können Sie Firewalls zwischen IaaS-Windows-Servern und SQL Server deaktivieren, sofern die Richtlinien der Site dies zulassen.

Tabelle 1-14. Eingehende Ports

Port	Protokoll	Komponente	Anmerkungen
443	TCP	Manager Service	Kommunikation mit IaaS-Komponenten und der vRealize Automation-Appliance über HTTPS
443	TCP	vRealize Automation-Appliance	Kommunikation mit IaaS-Komponenten und der vRealize Automation-Appliance über HTTPS

Tabelle 1-14. Eingehende Ports (Fortsetzung)

Port	Protokoll	Komponente	Anmerkungen
443	TCP	Infrastruktur-Endpoint-Hosts	Kommunikation mit IaaS-Komponenten und der vRealize Automation-Appliance über HTTPS. Normalerweise ist 443 der Standardkommunikationsport für virtuelle und Cloud-Infrastruktur-Endpoint-Hosts. Informieren Sie sich jedoch in der von Ihren Infrastruktur-Hosts bereitgestellten Dokumentation, um eine vollständige Liste von Standardports und erforderlichen Ports zu erhalten.
443	TCP	Gast-Agent Software-Bootstrap-Agent	Kommunikation mit Manager Service über HTTPS
443	TCP	DEM Worker	Kommunikation mit NSX Manager
1433	TCP	SQL Server-Instanz	MSSQL

Tabelle 1-15. Ausgehende Ports

Port	Protokoll	Komponente	Anmerkungen
53	TCP, UDP	Alle	DNS
67, 68, 546, 547	TCP, UDP	Alle	DHCP
123	TCP, UDP	Alle	Optional. NTP
443	TCP	Manager Service	Kommunikation mit der vRealize Automation-Appliance über HTTPS
443	TCP	Distributed Execution Manager	Kommunikation mit Manager Service über HTTPS
443	TCP	Proxy-Agents	Kommunikation mit Manager Service und Infrastruktur-Endpoint-Hosts über HTTPS
443	TCP	Management-Agent	Kommunikation mit der vRealize Automation-Appliance
443	TCP	Gast-Agent Software-Bootstrap-Agent	Kommunikation mit Manager Service über HTTPS
1433	TCP	Manager Service Website	MSSQL
5480	TCP	Alle	Kommunikation mit der vRealize Automation-Appliance.

Da Sie DTC zwischen allen Servern aktivieren, benötigt DTC Port 135 über TCP und einen zufälligen Port zwischen 1024 und 65535. Beachten Sie, dass anhand der Voraussetzungsprüfung überprüft wird, ob DTC ausgeführt und die erforderlichen Ports geöffnet sind.

IaaS -Webserver

Ein Windows-Server, der die Webkomponente hostet, muss neben den für alle IaaS Windows-Server geltenden Anforderungen zusätzliche Anforderungen erfüllen.

Unabhängig davon, ob die Webkomponente den Model Manager hostet oder nicht, sind die Anforderungen identisch.

- Konfigurieren Sie Java.
 - Installieren Sie Java 1.8, 64 Bit, Update 161 oder höher. Verwenden Sie nicht die 32-Bit-Version. Die JRE-Version ist ausreichend. Das vollständige JDK ist nicht notwendig.
 - Legen Sie die Umgebungsvariable JAVA_HOME auf den Java-Installationsordner fest.
 - Überprüfen Sie, ob die Datei %JAVA_HOME%\bin\java.exe verfügbar ist.
- Konfigurieren Sie Internet Information Services (IIS) entsprechend der folgenden Tabelle.

Sie benötigen IIS 7.5 für Windows 2008-Varianten, IIS 8 für Windows 2012, IIS 8.5 für Windows 2012 R2 und IIS 10 für Windows 2016.

Vermeiden Sie zusätzlich zu den Konfigurationseinstellungen das Hosting weiterer Websites in IIS. vRealize Automation legt die Bindung des Kommunikationsports für alle nicht zugewiesenen IP-Adressen fest, wodurch keine zusätzlichen Bindungen möglich sind. Der Standardkommunikationsport für vRealize Automation lautet 443.

Tabelle 1-16. IaaS -Manager Service-Host - Internet Information Services

IIS-Komponente	Einstellung
IIS-Rollen (Internet Information Services)	<ul style="list-style-type: none"> ■ Windows-Authentifizierung ■ Statische Inhalte ■ Standarddokument ■ ASPNET 3.5 und ASPNET 4.5 ■ ISAPI-Erweiterungen ■ ISAPI-Filter
IIS-Rollen des Windows-Prozessaktivierungsdiensts	<ul style="list-style-type: none"> ■ Konfigurations-API ■ Netzumgebung ■ Prozessmodell ■ WCF-Aktivierung (nur Windows 2008-Varianten) ■ HTTP-Aktivierung ■ Nicht-HTTP-Aktivierung (nur Windows 2008-Varianten) <p>(Windows 2012-Varianten: Wechseln Sie zu „Funktionen“ > „.Net Framework 3.5-Funktionen“ > „Nicht-HTTP-Aktivierung“.)</p>
IIS-Authentifizierungseinstellungen	<p>Legen Sie die folgenden Nicht-Standardwerte fest.</p> <ul style="list-style-type: none"> ■ Windows-Authentifizierung aktiviert ■ Anonyme Authentifizierung deaktiviert <p>Ändern Sie die folgenden Standardwerte nicht.</p> <ul style="list-style-type: none"> ■ Anbietershandlung aktiviert ■ NTLM-Anbieter aktiviert ■ Kernelmodus der Windows-Authentifizierung aktiviert ■ Erweiterter Schutz der Windows-Authentifizierung deaktiviert ■ Für Zertifikate, die SHA512 verwenden, muss TLS1.2 auf Windows 2012-Varianten deaktiviert werden.

IaaS -Manager Service-Host

Ein Windows-Server, der die Manager Service-Komponente hostet, muss neben den Anforderungen für alle IaaS-Windows-Server noch zusätzliche Anforderungen erfüllen.

Die Anforderungen sind identisch, gleich ob es sich bei dem Manager Service-Host um einen primären oder einen Backup-Host handelt.

- Zwischen einem Manager Service-Host und einem DEM-Host dürfen keine Firewalls vorhanden sein. Portinformationen finden Sie unter [Ports auf IaaS-Windows-Servern](#).
- Der Manager Service-Host muss den NetBIOS-Namen des SQL-Server-Datenbankhosts auflösen können. Wenn er den NetBIOS-Namen nicht auflösen kann, fügen Sie der Datei `/etc/hosts` der Manager Service-Maschine den NetBIOS-Namen des SQL-Servers hinzu.

IaaS SQL Server-Host

Ein Windows-Server, der die IaaS SQL-Datenbank hostet, muss bestimmte Anforderungen erfüllen.

Ihr SQL Server kann sich auf einem Ihrer IaaS Windows-Server oder auf einem separaten Host befinden. Wenn dieser gemeinsam mit IaaS-Komponenten gehostet wird, müssen neben diesen für alle IaaS Windows-Server geltenden Anforderungen zusätzliche Anforderungen erfüllt werden.

- Diese Version von vRealize Automation unterstützt nicht den standardmäßigen Kompatibilitätsmodus 130 für SQL Server 2016. Wenn Sie separat eine leere SQL Server 2016-Datenbank für die Verwendung mit IaaS erstellen, verwenden Sie den Kompatibilitätsmodus 100 oder 120.

Wenn Sie die Datenbank mit dem vRealize Automation-Installationsprogramm erstellen, ist die Kompatibilität bereits konfiguriert.

- AlwaysOn-Verfügbarkeitsgruppe (AlwaysOn Availability Group, AAG) wird nur für SQL Server 2016 Enterprise unterstützt. Bei Verwendung von AAG geben Sie den AAG-Listener-FQDN als SQL-Server-Host an.
- Wenn der SQL Server gemeinsam mit IaaS-Komponenten gehostet wird, konfigurieren Sie Java.
 - Installieren Sie Java 1.8, 64 Bit, Update 161 oder höher. Verwenden Sie nicht die 32-Bit-Version. Die JRE-Version ist ausreichend. Das vollständige JDK ist nicht notwendig.
 - Legen Sie die Umgebungsvariable `JAVA_HOME` auf den Java-Installationsordner fest.
 - Überprüfen Sie, ob die Datei `%JAVA_HOME%\bin\java.exe` verfügbar ist.
- Verwenden Sie eine unterstützte Version von SQL Server aus der [vRealize Automation-Support-Matrix](#).
- Aktivieren Sie das TCP/IP-Protokoll für SQL Server.
- SQL Server enthält eine Modelldatenbank, die als Vorlage für alle in der SQL-Instanz erstellten Datenbanken dient. Damit IaaS ordnungsgemäß installiert wird, ändern Sie nicht die Größe der Modelldatenbank.

- Im Gegensatz zu den in [IaaS-Windows-Server](#) aufgeführten Minimalanforderungen benötigt der Server in der Regel mehr Hardware.

Weitere Informationen finden Sie unter [vRealize Automation-Hardware-Spezifikationen und maximale Kapazitäten](#).

- Vor dem Ausführen des vRealize Automation-Installationsprogramms müssen Sie in der SQL-Instanz Konten angeben und Berechtigungen hinzufügen. Siehe [Konten und Kennwörter](#).

IaaS Distributed Execution Manager-Host

Ein Windows-Server, der die Orchestrator- oder die Worker-Komponente für Distributed Execution Manager (DEM) hostet, muss neben den Anforderungen für alle IaaS-Windows-Server noch zusätzliche Anforderungen erfüllen.

Zwischen einem DEM-Host und einem Manager Service-Host dürfen sich keine Firewalls befinden. Portinformationen finden Sie unter [Ports auf IaaS-Windows-Servern](#).

Für DEM-Worker gelten möglicherweise zusätzliche Anforderungen in Abhängigkeit von den Bereitstellungsressourcen, mit denen sie interagieren.

DEM-Worker mit Amazon Web Services

Ein vRealize Automation IaaS-DEM-Worker, der mit Amazon Web Services (AWS) kommuniziert, muss neben den allgemeinen Anforderungen für alle IaaS Windows-Server und DEMs noch zusätzliche Anforderungen erfüllen.

Ein DEM-Worker kann für die Bereitstellung mit AWS kommunizieren. Der DEM Worker kommuniziert mit einem Amazon EC2-Konto und erfasst Daten für dieses Konto.

- Der DEM-Worker benötigt Internetzugang.
- Wenn sich der DEM-Worker hinter einer Firewall befindet, muss der HTTPS-Datenverkehr zu und von `aws.amazon.com` zugelassen werden. Gleiches gilt für die URLs für EC2-Regionen, auf die Ihre AWS-Konten Zugriff haben, zum Beispiel `ec2.us-east-1.amazonaws.com` für die Region USA Ost. Jede URL wird in einen IP-Adressbereich aufgelöst. Deshalb müssen Sie diese IP-Adressen möglicherweise mit einem Tool wie dem auf der Network Solutions-Website verfügbaren Tool auflisten und konfigurieren.
- Wenn der DEM-Worker über einen Proxy-Server ins Internet gelangt, muss der DEM-Dienst unter Anmeldedaten ausgeführt werden, mit denen eine Authentifizierung beim Proxy-Server erfolgen kann.

DEM-Workern mit Openstack oder PowerVC

Ein vRealize Automation IaaS DEM-Worker, der mit Openstack oder PowerVC kommuniziert und Daten daraus erfasst, muss neben den Anforderungen für alle IaaS Windows-Server und DEM-Instanzen zusätzliche Anforderungen erfüllen.

Tabelle 1-17. Anforderungen für DEM-Worker mit Openstack und PowerVC

Ihre Installation	Anforderungen
Alle	<p>Aktivieren Sie in der Windows-Registrierung die Unterstützung von TLS v1.2 für .NET Framework. Beispiel:</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Windows 2008-DEM-Host	<p>Aktivieren Sie in der Windows-Registrierung das Protokoll TLS v1.2. Beispiel:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
Selbstsignierte Zertifikate auf Ihrem Infrastruktur-Endpoint-Host	<p>Wenn Ihre PowerVC- oder OpenStack-Instanz keine vertrauenswürdigen Zertifikate verwendet, importieren Sie das SSL-Zertifikat aus Ihrer PowerVC- oder OpenStack-Instanz in die vertrauenswürdige Stammzertifizierungsstelle auf jedem IaaS-Windows-Server, auf dem Sie einen vRealize Automation-DEM installieren möchten.</p>

DEM-Worker mit Red Hat Enterprise Virtualization

Ein vRealize Automation IaaS DEM-Worker, der mit Red Hat Enterprise Virtualization (RHEV) kommuniziert und Daten daraus erfasst, muss neben den Anforderungen für alle IaaS Windows-Server und DEM-Instanzen zusätzliche Anforderungen erfüllen.

- Sie müssen jede RHEV-Umgebung mit der Domäne verbinden, die den DEM-Worker enthält.
- Die Anmeldedaten, die für die Verwaltung des Endpoints verwendet werden, welcher eine RHEV-Umgebung darstellt, müssen über Administratorrechte in der RHEV-Umgebung verfügen. Wenn Sie RHEV für die Bereitstellung verwenden, kommuniziert der DEM-Worker mit diesem Konto und ruft Daten daraus ab.
- Die Anmeldedaten müssen auch über ausreichende Berechtigungen zum Erstellen von Objekten auf den Hosts innerhalb der Umgebung verfügen.

DEM-Worker mit SCVMM

Ein vRealize Automation IaaS DEM-Worker, der virtuellen Maschinen über SCVMM (System Center Virtual Machine Manager) verwaltet, muss neben den Anforderungen für alle IaaS Windows-Server und DEM-Instanzen zusätzliche Anforderungen erfüllen.

- Installieren Sie den DEM-Worker auf derselben Maschine, auf der sich die SCVMM-Konsole befindet. Es empfiehlt sich, die SCVMM-Konsole auf einem separaten DEM-Worker zu installieren.

- Der DEM Worker muss Zugriff auf das SCVMM-PowerShell-Modul haben, das mit der Konsole installiert ist.
- Die PowerShell-Ausführungsrichtlinie muss auf „RemoteSigned“ oder „Nicht eingeschränkt“ festgelegt sein.

Geben Sie für die Prüfung der PowerShell-Ausführungsrichtlinie einen der folgenden Befehle in die PowerShell-Eingabeaufforderung ein:

```
help about_signing  
help Set-ExecutionPolicy
```

- Wenn sich DEM Worker in der Instanz nicht auf konformen Maschinen befinden, leiten Sie SCVMM-verbundenen Workflows mit Skill-Befehlen an konforme DEM Worker weiter.

vRealize Automation unterstützt keine Bereitstellungsumgebung, die eine private SCVMM-Cloud-Konfiguration verwendet. vRealize Automation kann derzeit keine Datenerfassung, Datenzuordnung oder Datenbereitstellung basierend auf privaten SCVMM-Clouds durchführen.

Die folgenden zusätzlichen Anforderungen gelten für SCVMM.

- vRealize Automation unterstützt SCVMM 2012 R2, das PowerShell 3 oder höher erfordert.
- Installieren Sie die SCVMM-Konsole, bevor Sie die DEM Worker von vRealize Automation installieren, die SCVMM-Arbeitselemente in Anspruch nehmen.

Wenn Sie die DEM Worker vor der SCVMM-Konsole installieren, werden Protokollfehler ähnlich dem folgenden Beispiel angezeigt.

```
Workflow „ScvmmEndpointDataCollection“ ist mit der folgenden Ausnahme fehlgeschlagen: Der Begriff „Get-VMMServer“ wurde nicht als Name eines Cmdlet, eines ausführbaren Programms, einer Funktion oder Skriptdatei erkannt. Überprüfen Sie die Schreibweise des Namens oder, sofern ein Pfad einbezogen war, stellen Sie sicher, dass der Pfad korrekt ist, und versuchen Sie es erneut.
```

Um das Problem zu beheben, stellen Sie sicher, dass die SCVMM-Konsole installiert ist, und starten Sie den DEM Worker-Dienst neu.

- Jede SCVMM-Instanz muss mit der Domäne verbunden sein, die den Server enthält.
- Die Anmeldedaten, die zur Verwaltung des die SCVMM-Instanz darstellenden Endpoints verwendet werden, müssen über Administratorrechte auf dem SCVMM-Server verfügen.

Die Anmeldedaten müssen auch auf den Hyper-V Servern innerhalb der Instanz über Administratorrechte verfügen.

- Zur Bereitstellung von Maschinen auf einer SCVMM-Ressource muss der vRealize Automation-Benutzer, der das Katalogelement anfordert, über die Administratorrolle innerhalb der SCVMM-Instanz verfügen.

- Bei Hyper-V Servern innerhalb einer zu verwaltenden SCVMM-Instanz muss es sich um Windows 2008 R2 SP1-Server handeln, auf denen Hyper-V installiert ist. Der Prozessor muss mit den notwendigen Virtualisierungserweiterungen .NET Framework 4.5.2 oder höher ausgestattet sein, und Windows Management Instrumentation (WMI) muss aktiviert sein.
- Um eine Generation-2-Maschine auf einer SCVMM 2012 R2-Ressource bereitzustellen, müssen Sie folgende Eigenschaften zu dem Blueprint hinzufügen.

```
Scvmm.Generation2 = true  
Hyperv.Network.Type = synthetic
```

Generation-2-Blueprints sollten über eine mit vorhandenen Daten zusammengestellte virtualHardDisk (vHDX) auf der Informationsseite des Blueprint Builds verfügen. Eine leere Seite führt dazu, dass die Generation-2-Bereitstellung fehlschlägt.

Weitere Informationen zur Vorbereitung der Bereitstellung von Maschinen finden Sie unter [Vorbereiten der SCVMM-Umgebung](#).

Zertifikate

vRealize Automation verwendet SSL-Zertifikate für die sichere Kommunikation zwischen IaaS-Komponenten und Instanzen der vRealize Automation-Appliance. Die Appliances und die Windows-Installationsmaschinen tauschen diese Zertifikate aus, um eine vertrauenswürdige Verbindung herzustellen. Sie können Zertifikate von einer internen oder externen Zertifizierungsstelle beziehen oder aber während des Bereitstellungsverfahrens für jede Komponente selbstsignierte Zertifikate erstellen.

Wichtige Informationen zu Fehlerbehebung, Unterstützung und Anforderungen bezüglich der Vertrauenswürdigkeit für Zertifikate finden Sie im [VMware-Knowledgebase-Artikel 2106583](#).

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.

Zertifikate können nach der Bereitstellung aktualisiert oder ersetzt werden. Beispielsweise könnte während der Erstbereitstellung ein Zertifikat ablaufen oder Sie möchten selbstsignierte Zertifikate verwenden. In diesem Fall können Sie Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle beziehen, bevor Sie mit Ihrer vRealize Automation-Implementierung in den Live-Modus wechseln.

Tabelle 1-18. Zertifikatimplementierungen

Komponente	Minimale Bereitstellung (keine Produktionsumgebung)	Verteilte Bereitstellung (bereit für Produktionsumgebung)
vRealize Automation-Appliance	Generieren Sie während der Appliance-Konfiguration ein selbstsigniertes Zertifikat.	Für jeden Appliance-Cluster können Sie ein Zertifikat von einer internen oder externen Zertifizierungsstelle verwenden. Zertifikate für Mehrfachverwendung und Platzhalterzertifikate werden unterstützt.
IaaS-Komponenten	Akzeptieren Sie während der Installation die generierten selbstsignierten Zertifikate oder wählen Sie die Unterdrückung von Zertifikaten aus.	Beziehen Sie ein Mehrfachverwendungszertifikat, wie beispielsweise ein SAN-Zertifikat, von einer internen oder externen Zertifizierungsstelle, der Ihr Webclient vertraut.

Zertifikatsketten

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

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

Schließen Sie beim Importieren von Zertifikaten die Kopfzeile BEGIN CERTIFICATE und die Fußzeile END CERTIFICATE für jedes Zertifikat ein.

Änderungen des Zertifikats bei Anpassung der vRealize Automation -Anmelde-URL

Wenn Sie möchten, dass sich Benutzer bei einem anderen URL-Namen als einem vRealize Automation-Appliance- oder Lastausgleichsdienst-Namen anmelden, lesen Sie die Schritte vor und nach der Installation von CNAME unter [Festlegen der vRealize Automation-Anmelde-URL auf einen benutzerdefinierten Namen](#).

vRealize Automation -Zertifikatsanforderungen

Wenn Sie Ihre eigenen Zertifikate mit vRealize Automation verwenden zu können, müssen die Zertifikate bestimmte Anforderungen erfüllen.

Unterstützte Zertifikatstypen

In vielen Organisationen werden Zertifikate von externen Zertifizierungsstellen entsprechend den Anforderungen des Unternehmens ausgestellt oder angefordert.

Die folgenden Anforderungen beziehen sich auf allgemeine Identitätsformat- und Zertifikatstypen mit typischen vRealize Automation-Bereitstellungen.

Zertifikatseigenschaft	Anforderungen
Hash-Algorithmus	SHA1, SHA2, (256, 584, 512)
Signaturalgorithmus	RSASSA-PKCS1_V1_5
Schlüssellänge	2084, 4096

Hinweis Die RSASSA-PSS-Signatur wird für vRealize Automation-Bereitstellungen nicht unterstützt. Diese Signatur ist die Standardeinstellung für eine Microsoft-Zertifizierungsstelle unter Windows 2012 R2. Die Signatur ist ein konfigurierbarer Parameter. Sie müssen daher sicherstellen, dass dieser bei Verwendung einer Microsoft-Zertifizierungsstelle entsprechend festgelegt ist.

Liste der unterstützten vRealize Automation -Zertifikate

Hash-Algorithmus	SHA1				SHA2-256			
	Signaturalgorithmus	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS
Schlüsselgröße	2048	4096	2048	4096	2048	4096	2048	4096
Von vRealize Automation unterstützt	Unterstützung bestätigt	Unterstützung bestätigt	Nicht unterstützt	Nicht unterstützt	Unterstützung bestätigt	Unterstützung bestätigt	Nicht unterstützt	Nicht unterstützt

Hash-Algorithmus	SHA2-384				SHA2-512			
	Signaturalgorithmus	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS
Schlüsselgröße	2048	4096	2048	4096	2048	4096	2048	4096
Von vRealize Automation unterstützt	Unterstützung bestätigt	Unterstützung bestätigt	Nicht unterstützt	Nicht unterstützt	Unterstützung bestätigt	Unterstützung bestätigt	Nicht unterstützt	Nicht unterstützt

Extrahieren von Zertifikaten und privaten Schlüsseln

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

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

Tabelle 1-19. Beispielzertifikatwerte und -befehle (openssl)

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

Bereitstellen der vRealize Automation -Appliance

Die vRealize Automation-Appliance wird als offene Virtualisierungsdatei geliefert, die Sie in einer vorhandenen virtualisierten Infrastruktur bereitstellen.

Informationen zur Bereitstellung der vRealize Automation -Appliance

Für alle Installationen ist zunächst eine bereitgestellte, aber nicht konfigurierte vRealize Automation-Appliance erforderlich, bevor sie mit einer der vRealize Automation-Installationsoptionen fortfahren.

- Der konsolidierte, browserbasierte Installationsassistent
- Separate browserbasierte Appliance-Konfiguration, gefolgt von separaten Windows-Installationen für IaaS-Server
- Befehlszeilenbasiertes Hintergrundinstallationsprogramm, das Eingaben von einer Answer-Datei akzeptiert
- Die Installations-REST-API, die JSON-formatierte Eingaben akzeptiert

Bereitstellen der vRealize Automation -Appliance

Bevor Sie die Installationspfade nutzen können, gibt vRealize Automation vor, dass Sie mindestens eine vRealize Automation-Appliance bereitstellen.

Um die Appliance zu erstellen, verwenden Sie den vSphere Client zum Herunterladen und Bereitstellen einer teilweise konfigurierten virtuellen Maschine aus einer Vorlage. Möglicherweise müssen Sie den Vorgang mehr als einmal durchführen, wenn Sie eine Unternehmensbereitstellung für Hochverfügbarkeit und Failover bereitstellen möchten. Eine solche Bereitstellung verfügt in der Regel über mehrere vRealize Automation-Appliances hinter einem Lastausgleichsdienst.

Voraussetzungen

- Melden Sie sich beim vSphere Client mit einem Benutzerkonto mit Berechtigungen zum Bereitstellen von OVF-Vorlagen in der Bestandsliste an.
- Laden Sie die `.ovf`- oder `.ova`-Datei der vRealize Automation-Appliance in ein Verzeichnis herunter, auf das der vSphere Client zugreifen kann.

Verfahren

- 1 Wählen Sie die vSphere-Option **OVF-Vorlage bereitstellen** aus.
- 2 Geben Sie den Pfad zur Datei `.ovf`- oder `.ova`-Datei der vRealize Automation-Appliance ein.
- 3 Überprüfen Sie die Einzelheiten der Vorlage.
- 4 Lesen und akzeptieren Sie die folgende Endbenutzer-Lizenzvereinbarung.
- 5 Geben Sie einen Namen für die Appliance und ein Verzeichnis für die Bestandsliste ein.

Verwenden Sie beim Bereitstellen von Appliances jeweils einen anderen Namen und verwenden Sie keine nicht-alphanumerischen Zeichen, wie zum Beispiel den Unterstrich (`_`), im Namen.

- 6 Wählen Sie den Host und den Cluster aus, in dem die Appliance gespeichert wird.
- 7 Wählen Sie den Ressourcenpool aus, in dem die Appliance gespeichert wird.
- 8 Wählen Sie den Speicher aus, der die Appliance hostet.
- 9 Wählen Sie ein Festplattenformat aus.

Thick-Formate verbessern die Leistung und Thin-Formate sparen Speicherplatz.

Das Format wirkt sich nicht auf die Größe der Appliance-Festplatte aus. Wenn eine Appliance mehr Speicherplatz für Daten benötigt, fügen Sie nach der Bereitstellung eine weitere Festplatte mithilfe von vSphere hinzu.

- 10 Wählen Sie ein Zielnetzwerk aus dem Dropdown-Menü aus.
- 11 Legen Sie die Appliance-Eigenschaften fest.

- a Geben Sie ein Root-Kennwort ein und bestätigen Sie es.

Mit den Anmeldedaten für das Root-Konto melden Sie sich bei der Benutzeroberfläche der browserbasierten Verwaltungsschnittstelle an, die von der Appliance oder der Befehlszeilenkonsole des Appliance-Betriebssystems gehostet wird.

- b Wählen Sie aus, ob Remote-SSH-Verbindungen zur Befehlszeilenkonsole zulässig sein sollen.

Das Deaktivieren von SSH ist sicherer, setzt jedoch voraus, dass Sie direkt in vSphere auf die Konsole zugreifen und nicht über einen separaten Terminalclient.

- c Geben Sie für **Hostname** den vollqualifizierten Domännennamen (FQDN) der Appliance ein.
Um optimale Ergebnisse zu erzielen, geben Sie den FQDN ein, auch wenn Sie DHCP verwenden.

Hinweis vRealize Automation unterstützt DHCP, für Produktbereitstellungen werden jedoch statische IP-Adressen empfohlen.

- d Wenn Sie unter „Netzwerkeigenschaften“ statische IP-Adressen verwenden, geben Sie die Werte für das Gateway, die Netzmaske und die DNS-Server ein. Sie müssen auch die IP-Adresse, den FQDN und Domäne für die Appliance selbst eingeben, wie im folgenden Beispiel dargestellt.

Abbildung 1-13. Eigenschaften der virtuellen Appliance - Beispiele

▼ Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change this status from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use DHCP. Leave blank to try to reverse look up the IP address if you use DHCP. <input type="text" value="va1.mycompany.com"/>
Initial root password	This will be used as an initial password for the root user account. You can change the password using the passwd command or from the appliance Web console). Enter password <input type="password" value="*****"/> Confirm password <input type="password" value="*****"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. <input type="text" value="12.34.56.79"/>
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. <input type="text" value="12.34.56.80, 12.34.56.81"/>
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. <input type="text" value="12.34.56.78"/>
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. <input type="text" value="255.255.254.0"/>

- 12 Je nach Konfiguration Ihrer Bereitstellung, vCenter Server-Instanz und Ihres DNS wählen Sie eines der folgenden Verfahren zum Abschließen der OVA-Bereitstellung und zum Einschalten der Appliance aus.
- Wenn Sie die Bereitstellung unter vSphere durchgeführt haben und auf der Seite „Bereit zum Abschließen“ die Option **Nach der Bereitstellung einschalten** verfügbar ist, führen Sie die folgenden Schritte durch.
 - a Wählen Sie **Nach der Bereitstellung einschalten** aus und klicken Sie auf **Beenden**.
 - b Nachdem die Bereitstellung der Datei in vCenter Server abgeschlossen ist, klicken Sie auf **Schließen**.
 - c Warten Sie, bis die virtuelle Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
 - Wenn Sie die Bereitstellung unter vSphere durchgeführt haben und auf der Seite „Bereit zum Abschließen“ die Option **Nach der Bereitstellung einschalten** nicht verfügbar ist, führen Sie die folgenden Schritte durch.
 - a Nachdem die Bereitstellung der Datei in vCenter Server abgeschlossen ist, klicken Sie auf **Schließen**.
 - b Schalten Sie die vRealize Automation-Appliance ein.
 - c Warten Sie, bis die virtuelle Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
 - d Vergewissern Sie sich, dass die vRealize Automation-Appliance bereitgestellt ist, indem Sie dessen FQDN anpingen. Wenn Sie die Appliance nicht anpingen können, starten Sie die virtuelle Maschine neu.
 - e Warten Sie, bis die virtuelle Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
 - Wenn Sie die vRealize Automation-Appliance für vCloud mithilfe von vCloud Director bereitgestellt haben, überschreibt vCloud möglicherweise das Kennwort, das Sie bei der OVA-Bereitstellung eingegeben haben. Führen Sie die folgenden Schritte durch, um das Überschreiben zu verhindern.
 - a Klicken Sie nach der Bereitstellung in vCloud Director auf Ihre vApp, um die vRealize Automation-Appliance anzuzeigen.
 - b Klicken Sie mit der rechten Maustaste auf die vRealize Automation-Appliance und wählen Sie **Eigenschaften** aus.
 - c Klicken Sie auf die Registerkarte **Gastbetriebssystem-Anpassungen**.
 - d Deaktivieren Sie unter **Kennwort zurücksetzen** die Option **Lokales Administratorkennwort zulassen** und klicken Sie auf **OK**.
 - e Schalten Sie die vRealize Automation-Appliance ein.
 - f Warten Sie, bis die virtuelle Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
- 13 Vergewissern Sie sich, dass die vRealize Automation-Appliance bereitgestellt ist, indem Sie dessen FQDN anpingen.

Nächste Schritte

- (Optional) Fügen Sie Netzwerkkarten hinzu. Siehe [Hinzufügen von Netzwerkkarten vor Ausführung des Installationsprogramms](#).
- Melden Sie sich bei der browserbasierten Verwaltungsschnittstelle an, um den konsolidierten Installationsassistenten auszuführen oder die Appliance manuell zu konfigurieren.

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

- Alternativ dazu können Sie die Anmeldung überspringen und die Vorteile einer automatischen oder API-basierten Installation von vRealize Automation nutzen.

Hinzufügen von Netzwerkkarten vor Ausführung des Installationsprogramms

vRealize Automation unterstützt mehrere Netzwerkkarten (NICs). Bevor Sie das Installationsprogramm ausführen, ist es möglich, Netzwerkkarten zur vRealize Automation-Appliance oder zum IaaS-Windows-Server hinzuzufügen.

Wenn Sie mehrere Netzwerkkarten hinzufügen möchten, bevor Sie den vRealize Automation-Installationsassistenten ausführen, fügen Sie diese nach der Bereitstellung in vCenter, jedoch vor dem Starten des Assistenten hinzu. Es kann unter anderem aus folgenden Gründen vorkommen, dass Sie zusätzliche Netzwerkkarten frühzeitig hinzufügen möchten:

- Sie möchten Benutzer- und Infrastrukturnetze trennen.
- Sie benötigen eine zusätzliche Netzwerkkarte, damit IaaS-Server einer Active Directory-Domäne beitreten können.

Weitere Informationen zu Szenarien mit mehreren Netzwerkkarten finden Sie in diesem [Blogbeitrag zum VMware Cloud Management](#).

Berücksichtigen Sie bei drei oder mehr Netzwerkkarten die folgenden Einschränkungen.

- VIDM benötigt Zugriff auf die Postgres-Datenbank und Active Directory.
- In einem HA-Cluster benötigt VIDM Zugriff auf die Lastausgleichsdienst-URL.
- Die vorangehenden VIDM-Verbindungen müssen über die ersten beiden Netzwerkkarten erfolgen.
- Netzwerkkarten nach der zweiten NIC dürfen nicht von VIDM verwendet oder erkannt werden.
- Netzwerkkarten nach der zweiten NIC dürfen nicht für die Verbindung mit Active Directory verwendet werden.

Verwenden Sie die erste oder zweite Netzwerkkarte, wenn Sie ein Verzeichnis in vRealize Automation konfigurieren.

Voraussetzungen

Stellen Sie die OVF und die virtuellen Windows-Maschinen der vRealize Automation-Appliance bereit, melden Sie sich aber nicht an und starten Sie den Installationsassistenten nicht.

Verfahren

- 1 Fügen Sie in vCenter Netzwerkkarten für jede vRealize Automation-Appliance hinzu.
 - a Klicken Sie mit der rechten Maustaste auf die neu bereitgestellte Appliance und wählen Sie **Einstellungen bearbeiten** aus.
 - b Fügen Sie VMXNETn-Netzwerkkarten hinzu.
 - c Wenn die Appliance eingeschaltet ist, starten Sie sie neu.

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

- 3 Konfigurieren Sie die Netzwerkkarten durch Ausführung des folgenden Befehls für jede Netzwerkkarte.

Achten Sie darauf, die Standard-Gateway-Adresse aufzunehmen. Sie können statische Routen konfigurieren, nachdem Sie diesen Vorgang beendet haben.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6) IPv4-address netmask gateway-v4-address
```

Beispiel:

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20  
255.255.255.0 192.168.100.1
```

- 4 Stellen Sie sicher, dass alle vRealize Automation-Knoten sich gegenseitig über DNS-Namen auflösen können.
- 5 Stellen Sie sicher, dass alle vRealize Automation-Knoten auf alle Lastausgleich-FQDNs für vRealize Automation-Komponenten zugreifen können.
- 6 Wenn Sie Split-Brain-DNS verwenden, stellen Sie sicher, dass alle vRealize Automation-Knoten und VIPs denselben FQDN in DNS für jede Knoten-IP und -VIP aufweisen.
- 7 Fügen Sie in vCenter Netzwerkkarten zu IaaS-Windows-Servern hinzu.
 - a Klicken Sie mit der rechten Maustaste auf den IaaS-Server und wählen Sie **Einstellungen bearbeiten** aus.
 - b Fügen Sie Netzwerkkarten zur virtuellen Maschine des IaaS-Servers hinzu.
- 8 Konfigurieren Sie in Windows die hinzugefügten IaaS-Server-NICs und deren IP-Adressen. Falls erforderlich, finden Sie weitere Informationen in der Microsoft-Dokumentation.

Nächste Schritte

- (Optional) Wenn Sie statische Routen benötigen, folgen Sie den Richtlinien in [Konfigurieren von statischen Routen](#), bevor Sie mit der Installation fortfahren.
- Melden Sie sich bei der browserbasierten Verwaltungsschnittstelle an, um den konsolidierten Installationsassistenten auszuführen oder die Appliance manuell zu konfigurieren.

<https://vrealize-automation-appliance-FQDN:5480>

- Alternativ dazu können Sie die Anmeldung überspringen und die Vorteile einer automatischen oder API-basierten Installation von vRealize Automation nutzen.

Installieren von vRealize Automation mit dem Installationsassistenten

Der vRealize Automation-Installationsassistent bietet eine einfache und schnelle Möglichkeit zum Installieren von Minimal- oder Unternehmensbereitstellungen.

Bevor Sie den Assistenten starten, stellen Sie zur Erfüllung der Voraussetzungen eine vRealize Automation-Appliance bereit und konfigurieren IaaS-Windows-Server. Der Installationsassistent wird angezeigt, wenn Sie sich zum ersten Mal bei der neu bereitgestellten vRealize Automation-Appliance anmelden.

- Um den Assistenten zu beenden und später zu ihm zurückzukehren, klicken Sie auf **Abmelden**.
- Um den Assistenten zu deaktivieren, klicken Sie auf **Abbrechen** oder melden Sie sich ab und beginnen Sie mit der manuellen Installation über die Standardschnittstellen.

Der Assistent ist Ihr primäres Tool für neue vRealize Automation-Installationen. Wenn Sie eine vorhandene vRealize Automation-Bereitstellung nach dem Ausführen des Assistenten erweitern möchten, finden Sie Informationen zu den dafür geeigneten Verfahren unter [Die vRealize Automation-Standard-Installationsschnittstellen](#).

Verwenden des Installationsassistenten für minimale Bereitstellungen

Minimalbereitstellungen zeigen, wie vRealize Automation funktioniert, haben jedoch normalerweise nicht die Kapazität, Produktionsumgebungen von Unternehmen zu unterstützen.

Installieren Sie eine Minimalbereitstellung für Proof-of-Concept-Zwecke oder um sich mit vRealize Automation vertraut zu machen.

Starten des Installationsassistenten für eine Minimalbereitstellung

Minimalbereitstellungen bestehen üblicherweise aus einer vRealize Automation-Appliance, einem IaaS Windows-Server und dem vSphere-Agent für Endpoints. Die Minimalinstallation speichert alle IaaS-Komponenten auf einem einzigen Windows-Server.

Voraussetzungen

- Sorgen Sie dafür, dass die in [Vorbereitung für die Installation von vRealize Automation](#) erläuterten Voraussetzungen erfüllt sind.
- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).

Verfahren

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

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

- 2 Wenn der Installationsassistent angezeigt wird, klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite „Bereitstellungstyp“ **Minimalbereitstellung** und **Infrastructure as a Service installieren** und klicken Sie auf **Weiter**.
- 5 Melden Sie sich auf der Seite „Installationsvoraussetzungen“ bei den IaaS-Windows-Servern an und installieren den Management-Agent. Mit dem Management-Agent kann die vRealize Automation-Appliance die IaaS-Server erkennen und eine Verbindung zu ihnen herstellen.

Nächste Schritte

Installieren Sie den Management-Agent auf Ihrem IaaS-Windows-Server. Siehe [Installieren des vRealize Automation-Management-Agents](#).

Installieren des vRealize Automation -Management-Agents

Alle IaaS-Windows-Server benötigen den Management-Agent, der sie mit ihrer jeweiligen vRealize Automation-Appliance verbindet.

Wenn Sie die SQL Server-Datenbank von vRealize Automation auf einem separaten Windows-Rechner hosten, der keine IaaS-Komponenten hostet, ist für die SQL Server-Maschine kein Management-Agent erforderlich.

Der Management-Agent registriert den IaaS-Windows-Server bei der jeweiligen vRealize Automation-Appliance, automatisiert die Installation und Verwaltung von IaaS-Komponenten und erfasst Support- und Telemetriedaten. Der Management-Agent wird als Windows-Dienst unter einem Domänenkonto mit Administratorrechten für IaaS-Windows-Server ausgeführt.

Voraussetzungen

Erstellen Sie eine vRealize Automation-Appliance und starten Sie den Installationsassistenten.

Siehe [Bereitstellen der vRealize Automation-Appliance](#) und [Starten des Installationsassistenten für eine Minimalbereitstellung](#).

Verfahren

- 1 Melden Sie sich bei der Konsole der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Geben Sie den folgenden Befehl ein:

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Kopieren Sie den Fingerabdruck zwecks späterer Überprüfung. Beispiel:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Melden Sie sich beim IaaS-Windows-Server mit einem Konto mit Administratorrechten an.
- 5 Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance in einem Webbrowser.

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

- 6 Klicken Sie auf **Installationsprogramm für den Management-Agent** und speichern Sie die .msi-Datei und führen Sie sie aus.
- 7 Lesen Sie die Begrüßungsseite.
- 8 Akzeptieren Sie die Lizenzvereinbarung für Endbenutzer.
- 9 Übernehmen oder ändern Sie den Installationsordner.
Programme (x86)\VMware\VCAC\Management Agent
- 10 Geben Sie die Details der vRealize Automation-Appliance ein:
 - a Geben Sie die Appliance HTTPS-Adresse, einschließlich FQDN und :5480-Portnummer ein.
 - b Geben Sie die Anmeldedaten für das Root-Konto der Appliance ein.
 - c Klicken Sie auf **Laden** und bestätigen Sie, dass der Fingerabdruck mit demjenigen übereinstimmt, den Sie zuvor kopiert haben. Ignorieren Sie Doppelpunkte.

Wenn die Fingerabdrücke nicht übereinstimmen, stellen Sie sicher, dass Sie über die richtige Appliance-Adresse verfügen.

Abbildung 1-14. Management-Agent – Details zur vRealize Automation-Appliance

vRA appliance address:
https://va1.company.com:5480
Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5480
Root username: root Password:
Provide vRealize Automation appliance root user credentials
Management Site Service certificate SHA1 fingerprint:
718447720357C8C268650006BCD823989254BF89 Load
 I confirm the fingerprint matches the Management Site Service SSL certificate

- 11 Geben Sie die Domäne bzw. den Benutzernamen und das Kennwort für das Dienstkonto ein.
Das Dienstkonto muss ein Domänenkonto mit Administratorrechten auf IaaS-Windows-Servern sein. Verwenden Sie durchgängig dasselbe Dienstkonto.
- 12 Folgen Sie den Anweisungen zum Abschließen der Installation des Management-Agents.

Hinweis Da diese verknüpft sind, müssen Sie den Management-Agent neu installieren, wenn Sie die vRealize Automation-Appliance ersetzen.

Bei der Deinstallation von IaaS auf einem Windows-Server wird der Management-Agent nicht entfernt. Um einen Management-Agent zu deinstallieren, verwenden Sie die Option zum Hinzufügen oder Entfernen von Programmen in Windows.

Nächste Schritte

Kehren Sie zum browserbasierten Installationsassistenten zurück. IaaS-Windows-Server mit installiertem Management-Agent werden unter „Erkannte Hosts“ angezeigt.

Abschließen des Installationsassistenten

Wechseln Sie nach der Installation des Management-Agenten wieder zum Assistenten und befolgen Sie die Eingabeaufforderungen. Wenn Sie weitere Anweisungen zu den Einstellungen benötigen, klicken Sie auf den Hilfe-Link oben rechts im Assistenten.

- Nachdem Sie den Assistenten abgeschlossen haben, werden auf der letzten Seite der Pfad und der Name einer Eigenschaftsdatei angezeigt. Sie können die Datei bearbeiten und sie zum Durchführen einer automatischen vRealize Automation-Installation mit denselben oder ähnlichen Einstellungen von Ihrer Assistentensitzung aus verwenden. Siehe [Automatische Installation von vRealize Automation](#).
- Wenn Sie anfängliche Inhalte erstellt haben, können Sie sich bei dem Standardmandanten als Benutzer „configurationadmin“ anmelden und die Katalogelemente anfordern. Ein Beispiel zum Anfordern des Elements und zum Abschließen der manuellen Benutzeraktion finden Sie unter: [Szenario: Anfordern anfänglicher Inhalte für eine Rainpole-Proof-of-Concept-Bereitstellung](#).
- Informationen zum Konfigurieren des Zugriffs auf den Standardmandanten finden Sie unter [Konfigurieren des Zugriffs auf den Standardmandanten](#).

Verwenden des Installationsassistenten für Unternehmensbereitstellungen

Ihre Unternehmensbereitstellung können Sie an die Anforderungen Ihres Unternehmens anpassen. Eine Unternehmensbereitstellung kann aus verteilten Komponenten oder High Availability-Bereitstellungen mit konfigurierten Lastausgleichsdiensten bestehen.

Unternehmensbereitstellungen sind für komplexere Installationsstrukturen mit verteilten und redundanten Komponenten konzipiert und enthalten im Allgemeinen Lastausgleichsdienste. Die Installation von IaaS-Komponenten ist bei beiden Bereitstellungstypen optional.

Für Bereitstellungen mit Lastausgleichsdienst verursachen mehrere aktive Webserverinstanzen und vRealize Automation-Appliances ein Fehlschlagen der Installation. Nur eine einzige Webserverinstanz und eine vRealize Automation-Appliance dürfen während der Installation aktiv sein.

Starten des Installationsassistenten für eine Unternehmensbereitstellung

Unternehmensbereitstellungen sind groß genug für Produktionsumgebungen. Mit dem Installationsassistenten können Sie eine verteilte Installation oder eine verteilte Installation mit Lastausgleichsdiensten zur Unterstützung von Hochverfügbarkeit und Failover bereitstellen.

Wenn Sie eine verteilte Installation mit Lastausgleichsdiensten bereitstellen, benachrichtigen Sie das Team, das für die Konfiguration Ihrer vRealize Automation-Umgebung verantwortlich ist. Ihre Mandantadministratoren müssen die Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren, wenn sie den Link zu Active Directory konfigurieren.

Voraussetzungen

- Sorgen Sie dafür, dass die in [Vorbereitung für die Installation von vRealize Automation](#) erläuterten Voraussetzungen erfüllt sind.
- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).

Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Wenn der Installationsassistent angezeigt wird, klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Anwender-Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite „Bereitstellungstyp“ **Unternehmensbereitstellung** und **Infrastructure as a Service installieren** aus.
- 5 Melden Sie sich auf der Seite „Installationsvoraussetzungen“ bei den IaaS-Windows-Servern an und installieren den Management-Agent. Mit dem Management-Agent kann die vRealize Automation-Appliance diese IaaS-Server erkennen und eine Verbindung zu ihnen herstellen.

Nächste Schritte

Installieren Sie den Management-Agent auf den IaaS-Windows-Servern. Siehe [Installieren des vRealize Automation-Management-Agents](#).

Installieren des vRealize Automation -Management-Agents

Alle IaaS-Windows-Server benötigen den Management-Agent, der sie mit ihrer jeweiligen vRealize Automation-Appliance verbindet.

Wenn Sie die SQL Server-Datenbank von vRealize Automation auf einem separaten Windows-Rechner hosten, der keine IaaS-Komponenten hostet, ist für die SQL Server-Maschine kein Management-Agent erforderlich.

Der Management-Agent registriert den IaaS-Windows-Server bei der jeweiligen vRealize Automation-Appliance, automatisiert die Installation und Verwaltung von IaaS-Komponenten und erfasst Support- und Telemetriedaten. Der Management-Agent wird als Windows-Dienst unter einem Domänenkonto mit Administratorrechten für IaaS-Windows-Server ausgeführt.

Voraussetzungen

Erstellen Sie eine vRealize Automation-Appliance und starten Sie den Installationsassistenten.

Siehe [Bereitstellen der vRealize Automation-Appliance](#) und [Starten des Installationsassistenten für eine Unternehmensbereitstellung](#).

Verfahren

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

- 2 Geben Sie den folgenden Befehl ein:

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

- 3 Kopieren Sie den Fingerabdruck zwecks späterer Überprüfung. Beispiel:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```

- 4 Melden Sie sich beim IaaS-Windows-Server mit einem Konto mit Administratorrechten an.
5 Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance in einem Webbrowser.

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

- 6 Klicken Sie auf **Installationsprogramm für den Management-Agent** und speichern Sie die .msi-Datei und führen Sie sie aus.

- 7 Lesen Sie die Begrüßungsseite.

- 8 Akzeptieren Sie die Lizenzvereinbarung für Endbenutzer.

- 9 Übernehmen oder ändern Sie den Installationsordner.

```
Programme (x86)\VMware\VCAC\Management Agent
```

- 10 Geben Sie die Details der vRealize Automation-Appliance ein:

- a Geben Sie die Appliance HTTPS-Adresse, einschließlich FQDN und :5480-Portnummer ein.
- b Geben Sie die Anmeldedaten für das Root-Konto der Appliance ein.
- c Klicken Sie auf **Laden** und bestätigen Sie, dass der Fingerabdruck mit demjenigen übereinstimmt, den Sie zuvor kopiert haben. Ignorieren Sie Doppelpunkte.

Wenn die Fingerabdrücke nicht übereinstimmen, stellen Sie sicher, dass Sie über die richtige Appliance-Adresse verfügen.

Abbildung 1-15. Management-Agent - Details zur vRealize Automation-Appliance

vRA appliance address:

Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5480

Root username: Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

I confirm the fingerprint matches the Management Site Service SSL certificate

11 Geben Sie die Domäne bzw. den Benutzernamen und das Kennwort für das Dienstkonto ein.

Das Dienstkonto muss ein Domänenkonto mit Administratorrechten auf IaaS-Windows-Servern sein. Verwenden Sie durchgängig dasselbe Dienstkonto.

12 Folgen Sie den Anweisungen zum Abschließen der Installation des Management-Agents.

Wiederholen Sie den Vorgang für alle Windows-Server, auf denen IaaS-Komponenten gehostet werden.

Hinweis Da diese verknüpft sind, müssen Sie den Management-Agent neu installieren, wenn Sie die vRealize Automation-Appliance ersetzen.

Bei der Deinstallation von IaaS auf einem Windows-Server wird der Management-Agent nicht entfernt. Um einen Management-Agent zu deinstallieren, verwenden Sie die Option zum Hinzufügen oder Entfernen von Programmen in Windows.

Nächste Schritte

Kehren Sie zum browserbasierten Installationsassistenten zurück. IaaS-Windows-Server mit installiertem Management-Agent werden unter „Erkannte Hosts“ angezeigt.

Abschließen des Installationsassistenten

Wechseln Sie nach der Installation des Management-Agenten wieder zum Assistenten und befolgen Sie die Eingabeaufforderungen. Wenn Sie weitere Anweisungen zu den Einstellungen benötigen, klicken Sie auf den Hilfe-Link oben rechts im Assistenten.

- Nachdem Sie den Assistenten abgeschlossen haben, werden auf der letzten Seite der Pfad und der Name einer Eigenschaftsdatei angezeigt. Sie können die Datei bearbeiten und sie zum Durchführen einer automatischen vRealize Automation-Installation mit denselben oder ähnlichen Einstellungen von Ihrer Assistentensitzung aus verwenden. Siehe [Automatische Installation von vRealize Automation](#).
- Wenn Sie anfängliche Inhalte erstellt haben, können Sie sich bei dem Standardmandanten als Benutzer „configurationadmin“ anmelden und die Katalogelemente anfordern. Ein Beispiel zum Anfordern des Elements und zum Abschließen der manuellen Benutzeraktion finden Sie unter: [Szenario: Anfordern anfänglicher Inhalte für eine Rainpole-Proof-of-Concept-Bereitstellung](#).
- Informationen zum Konfigurieren des Zugriffs auf den Standardmandanten finden Sie unter [Konfigurieren des Zugriffs auf den Standardmandanten](#).

Befolgen der Anweisungen des vRealize Automation -Installationsassistenten

Der vRealize Automation-Installationsassistent stellt Ihnen benutzerfreundliche Seiten bereit, anhand derer Sie Voraussetzungen suchen, Einstellungen eingeben, Einstellungen überprüfen und vRealize Automation-Komponenten installieren können.

Hinweis Der Assistent enthält Schritte, mit denen Sie sich bei anderen Systemen (z. B. Lastausgleichsdiensten oder IaaS-Windows-Servern) anmelden.

Voraussetzungen

- Erstellen Sie eine oder mehrere nicht konfigurierte Appliances. Siehe [Bereitstellen der vRealize Automation-Appliance](#).

Minimalbereitstellungen verwenden eine vRealize Automation-Appliance. Unternehmensbereitstellungen können hinter dem Lastausgleich mehrere Appliances aufweisen.

- Halten Sie mindestens ein Windows-System verfügbar, auf dem die IaaS-Komponenten gehostet werden können.
- Starten Sie den Assistenten, indem Sie sich als Root-Benutzer bei der Verwaltungsschnittstelle der vRealize Automation-Appliance anmelden.

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

Verfahren

1 [Bereitstellungstyp](#)

Auf der Seite „Bereitstellungstyp“ entscheiden Sie, welche und wie viele der einzelnen vRealize Automation-Komponenten Sie installieren.

2 [Installationsvoraussetzungen](#)

Auf der Seite „Installationsvoraussetzungen“ richten Sie eine Verbindung zu den Windows-Maschinen ein, die vRealize Automation IaaS hosten. Darüber hinaus wählen Sie eine Quelle für die Zeitsynchronisierung aus.

3 [vRealize-Appliances](#)

(Nur Unternehmensbereitstellungen) Auf der Seite „vRealize-Appliances“ haben Sie die Möglichkeit, eine Hochverfügbarkeitsbereitstellung mit mehreren vRealize Automation-Appliances zu erstellen.

4 [Serverrollen](#)

(Nur Unternehmensbereitstellungen) Auf der Seite „Serverrollen“ weisen Sie vRealize Automation IaaS-Komponentenrollen den Windows-Maschinen zu, auf denen Sie zuvor den Management-Agent installiert haben.

5 [Voraussetzungsprüfung](#)

Auf der Seite „Voraussetzungsprüfung“ überprüfen und korrigieren Sie Ihre Windows-Server mit vRealize Automation zur Unterstützung der IaaS-Installation.

6 [vRealize Automation-Host](#)

Auf der Seite „vRealize Automation-Host“ legen Sie die Basis-URL-Adresse für vRealize Automation fest. Die Adresse ist in der Regel die vRealize Automation-Appliance oder in Hochverfügbarkeitsbereitstellungen ein Lastausgleichsdienst.

7 [Single Sign On](#)

Auf der Seite „Single Sign On“ legen Sie die Anmeldedaten für den Systemadministrator des vRealize Automation-Standardmandanten fest.

8 IaaS-Host

Auf der IaaS-Host-Seite legen Sie die URL-Basisadressen für bestimmte IaaS-Komponenten fest. Darüber hinaus erstellen Sie eine Sicherheits-Passphrase für die vRealize Automation IaaS-SQL-Datenbank.

9 Microsoft SQL Server

Auf der Seite „Microsoft SQL Server“ konfigurieren Sie die vRealize Automation IaaS-SQL-Datenbank. In der IaaS-Datenbank werden bereitgestellte Maschinen, zugeordnete Elemente und Richtlinien erfasst.

10 Webrolle

(Nur Unternehmensbereitstellungen) Auf der Seite „Webrolle“ konfigurieren Sie die vRealize Automation IaaS-Website separat in IIS.

11 Manager Service-Rolle

(Nur Unternehmensbereitstellungen) Auf der Seite „Manager Service-Rolle“ konfigurieren Sie die separate vRealize Automation-Windows-Maschine, die den IaaS Manager Service hostet.

12 Distributed Execution Manager

Auf der Seite „Distributed Execution Manager“ konfigurieren Sie die vRealize Automation-Windows-Maschinen, die IaaS-DEMs hosten. Es werden mehrere DEM-Hosts unterstützt.

13 Agents

Auf der Seite „Agenten“ erstellen Sie die Verknüpfung zwischen vRealize Automation IaaS und den Virtualisierungsressourcen, auf denen die Infrastruktur bereitgestellt wird. Sie wählen einen Agent-Typ aus und geben die Details für den entsprechenden Endpoint an.

14 vRealize Appliance-Zertifikat

Auf der Seite „vRealize Appliance-Zertifikat“ erstellen Sie das von der vRealize Automation-Appliance verwendete Authentifizierungszertifikat oder wählen es aus. Wenn das Zertifikat selbstsigniert ist, wird es Endbenutzern angezeigt, und sie bestätigen es, wenn sie sich in einem Browser bei vRealize Automation anmelden.

15 Webzertifikat

Auf der Seite „Webzertifikat“ erstellen Sie das vom IaaS-Webserver verwendete Authentifizierungszertifikat oder wählen es aus. Die vRealize Automation-Appliance stellt eine Verbindung zum Webserver her und muss ihn authentifizieren und ihm vertrauen.

16 Manager Service-Zertifikat

(Nur Unternehmensbereitstellungen) Auf der Seite „Manager Service-Zertifikat“ erstellen Sie das vom vRealize Automation IaaS Manager Service-Host verwendete Authentifizierungszertifikat oder wählen es aus. Die anderen IaaS-Windows-Server stellen eine Verbindung zum Manager Service-Host her und müssen ihn authentifizieren und ihm vertrauen.

17 Lastausgleichsdienste

(Nur Unternehmensbereitstellungen) Auf der Seite „Lastausgleichsmodule“ halten Sie die Konfiguration von Lastausgleichsdiensten für den richtigen Pool von vRealize Automation-Mitgliedssystemen an.

18 Validierung

Auf der Seite „Validierung“ stellen Sie sicher, dass die vRealize Automation-Installation fortgesetzt werden kann.

19 Snapshots erstellen

Auf der Seite „Snapshots erstellen“ erstellen Sie VM-Snapshots von allen vRealize Automation-Komponenten, bevor Sie mit der Installation fortfahren.

20 Installationsdetails

Auf der Seite „Installationsdetails“ starten Sie die vRealize Automation-Installation oder wiederholen sie, falls Probleme aufgetreten sind.

21 Lizenzierung

Auf der Seite „Lizenzierung“ geben Sie einen Schlüssel ein, um das installierte vRealize Automation-Produkt zu aktivieren.

22 Telemetrie

Auf der Seite „Telemetrie“ entscheiden Sie, ob vRealize Automation im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit Nutzungsstatistiken an VMware sendet.

23 Optionen nach der Installation

Auf der Seite „Optionen nach der Installation“ stehen Optionen zum Erstellen neuer vRealize Automation-Daten oder Migrieren älterer Bereitstellungsdaten auf die neue Installation zur Verfügung.

24 Konfiguration von anfänglichen Inhalten

Auf der Seite „Konfiguration von anfänglichen Inhalten“ erstellen Sie einen neuen lokalen vRealize Automation-Standardmandantenbenutzer, der einen Inhaltsworkflow für einen vSphere-Endpoint beginnen kann.

25 Migrationskonfiguration

Auf der Seite „Migrationskonfiguration“ können Sie die Übertragung von einer anderen, älteren vRealize Automation-Bereitstellung an die neu installierte Bereitstellung starten.

Bereitstellungstyp

Auf der Seite „Bereitstellungstyp“ entscheiden Sie, welche und wie viele der einzelnen vRealize Automation-Komponenten Sie installieren.

Minimal

Minimalbereitstellungen verwenden nur eine vRealize Automation-Appliance und einen Windows-Server, der IaaS-Komponenten hostet. Bei minimalen Bereitstellungen können Sie die IaaS-Datenbank auf einem separaten SQL Server-System hosten oder SQL auf dem IaaS-Windows-Server installieren.

Eine Minimalbereitstellung kann nicht in eine Unternehmensbereitstellung konvertiert werden. Beginnen Sie zum Hochskalieren einer Bereitstellung mit einer kleinen Unternehmensbereitstellung und fügen Sie darin Komponenten hinzu. Eine Minimalbereitstellung wird als Ausgangspunkt nicht unterstützt.

Enterprise

Unternehmensbereitstellungen umfassen mehrere separate Appliances und Windows-Hosts mit Lastausgleich. In Unternehmensbereitstellungen ist es zudem möglich, die IaaS-Datenbank auf einem separaten SQL Server-System oder auf einem der IaaS-Windows-Server zu hosten.

Wenn Sie eine Unternehmensbereitstellung auswählen, werden in der Übersichtsliste links im Assistenten zusätzliche Seiten des Installationsassistenten angezeigt.

Infrastructure as a Service

Mit der Option „Infrastructure as a Service“ (IaaS) geben Sie an, ob Sie vorhandene Windows-Maschinen mit Modellierungs- und Bereitstellungsfunktionen von vRealize Automation konfigurieren oder nicht.

Wenn Sie „IaaS“ auswählen, werden in der Übersichtsliste links im Assistenten zusätzliche Seiten des Installationsassistenten angezeigt.

Installationsvoraussetzungen

Auf der Seite „Installationsvoraussetzungen“ richten Sie eine Verbindung zu den Windows-Maschinen ein, die vRealize Automation IaaS hosten. Darüber hinaus wählen Sie eine Quelle für die Zeitsynchronisierung aus.

IaaS -Windows-Server

Damit eine Windows-Maschine als IaaS-Komponentenhost dienen kann, müssen Sie vCAC-IaaSManagementAgent-Setup.msi auf die Windows-Maschine herunterladen und dort installieren.

Die Management-Agent-Installation muss mit einer ausgeführten vRealize Automation-Appliance kommunizieren können. Bei jeder Installation des Management-Agents unter Windows wird das jeweilige System eindeutig an die bestimmte Appliance und Bereitstellung gebunden.

Potenzielle IaaS-Windows-Server, auf denen der richtige Management-Agent installiert ist, werden unter **Erkannte Hosts** angezeigt.

Klicken Sie auf **Löschen**, damit der Installationsassistent einen erkannten Host ignoriert. Beim Löschen eines Windows-Hosts wird der zugehörige Management-Agent nicht entfernt. Zum Deinstallieren des Agents verwenden Sie die Funktion „Software“ direkt in Windows.

Zeitquelle

Sie müssen alle vRealize Automation-Appliances und IaaS-Windows-Server mit derselben Zeitquelle synchronisieren. Die folgenden Quellen sind zulässig:

- Hostzeit verwenden – Die Synchronisierung wird mit dem ESXi-Host der vRealize Automation-Appliance durchgeführt.

- Zeitserver verwenden – Die Synchronisierung erfolgt mit einem externen NTP-Server (Network Time Protocol). Geben Sie den FQDN oder die IP-Adresse des NTP-Servers ein.

Verwenden Sie innerhalb einer vRealize Automation-Bereitstellung niemals verschiedene Zeitquellen.

vRealize-Appliances

(Nur Unternehmensbereitstellungen) Auf der Seite „vRealize-Appliances“ haben Sie die Möglichkeit, eine Hochverfügbarkeitsbereitstellung mit mehreren vRealize Automation-Appliances zu erstellen.

Mehrere Appliances müssen hinter einem separat installierten Lastausgleich gehostet werden. Auf einer der nachfolgenden Seiten des Assistenten überprüfen und schließen Sie die Konfiguration der Appliances und des Lastausgleichsdiensts ab. Geben Sie für jede von Ihnen hinzugefügte vRealize Automation-Appliance den zugehörigen FQDN und die Root-Anmeldedaten ein.

Serverrollen

(Nur Unternehmensbereitstellungen) Auf der Seite „Serverrollen“ weisen Sie vRealize Automation IaaS-Komponentenrollen den Windows-Maschinen zu, auf denen Sie zuvor den Management-Agent installiert haben.

IaaS-Windows-Maschinen können als primäre und zusätzliche Webserver, Manager Service-Hosts, DEM-Hosts und Agent-Hosts genutzt werden. Weitere Informationen zu IaaS-Komponentenrollen finden Sie unter [Infrastructure as a Service](#).

Die Trennung der IaaS Serverrollen ist nur in Unternehmensbereitstellungen möglich. Bei minimalen Bereitstellungen übernimmt eine Windows-Maschine alle Rollen.

Voraussetzungsprüfung

Auf der Seite „Voraussetzungsprüfung“ überprüfen und korrigieren Sie Ihre Windows-Server mit vRealize Automation zur Unterstützung der IaaS-Installation.

Die Voraussetzungsprüfung überprüft die Windows-Maschinen, auf denen Sie den Management-Agent installiert haben, und hostet IaaS-Komponenten. Zu den Voraussetzungen zählen u. a. Java, die IIS-Einstellungen (Internet Information Services) und der DTC-Dienst (Microsoft Distributed Transaction Coordinator). Klicken Sie auf **Details anzeigen**, um eine Liste der Voraussetzungen anzuzeigen.

Bei Verwendung des Installationsassistenten können Sie ohne Überprüfung der Voraussetzungen fortfahren. Beachten Sie aber, dass die Installation möglicherweise fehlschlägt.

- Klicken Sie auf **Ausführen**, um die Voraussetzungen zu prüfen.
- Wenn erforderliche Komponenten fehlen, klicken Sie auf **Details anzeigen**, um weitere Informationen zu erhalten. Klicken Sie dann auf **Korrigieren**.

Der Installationsassistent kann die meisten software- oder einstellungsbasierten Voraussetzungen korrigieren. Nachdem Sie die gewünschten Änderungen vorgenommen haben, führt der Installationsassistent einen Neustart Ihrer IaaS-Hosts durch.

Der Assistent kann Probleme aufgrund von nicht genügend Arbeitsspeicher oder unzureichenden CPU-Ressourcen nicht beheben. Probleme dieser Art müssen Sie gegebenenfalls in vSphere oder auf Ihrer Hardware beheben.

vRealize Automation -Host

Auf der Seite „vRealize Automation-Host“ legen Sie die Basis-URL-Adresse für vRealize Automation fest. Die Adresse ist in der Regel die vRealize Automation-Appliance oder in Hochverfügbarkeitsbereitstellungen ein Lastausgleichsdienst.

- Wenn Sie nur eine vRealize Automation-Appliance ohne Lastausgleich bereitstellen, geben Sie den FQDN der vRealize Automation-Appliance ein. Sie können klicken, damit der Installationsassistent den FQDN für Sie auffüllt.
- Wenn Sie eine Unternehmenskonfiguration bereitstellen, die eine oder mehrere vRealize Automation -Appliances hinter dem Lastausgleichsdienst enthält, geben Sie stattdessen den FQDN des Lastausgleichsdiensts ein.

Auch eine einzelne vRealize Automation-Appliance kann hinter einem Lastausgleichsdienst bereitgestellt werden. Bei diesem Ansatz können Sie Appliances später problemlos hinzufügen, wenn Sie die Bereitstellung erweitern möchten.

Single Sign On

Auf der Seite „Single Sign On“ legen Sie die Anmeldedaten für den Systemadministrator des vRealize Automation-Standardmandanten fest.

Der Systemadministrator des Standardmandanten besitzt von allen Benutzern die meisten Berechtigungen, einschließlich der Berechtigung zum Erstellen zusätzlicher Mandanten. Die Anmeldedaten für den Systemadministrator des Standardmandanten unterscheiden sich von den Root-Anmeldedaten der vRealize Automation-Appliance.

IaaS -Host

Auf der IaaS-Host-Seite legen Sie die URL-Basisadressen für bestimmte IaaS-Komponenten fest. Darüber hinaus erstellen Sie eine Sicherheits-Passphrase für die vRealize Automation IaaS-SQL-Datenbank.

Minimalbereitstellungen

Einstellung	Beschreibung
IaaS-Web-Adresse	Geben Sie den FQDN des IaaS-Windows-Servers ein.
Installieren von IaaS-Komponenten auf	Wählen Sie den FQDN des IaaS Windows-Servers aus oder geben Sie ihn ein.
Username	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.
Password	Geben Sie das Kennwort des Kontos ein.
Sicherheitskennwortsatz	Erstellen Sie eine Passphrase, um Daten in der IaaS-SQL-Datenbank zu verschlüsseln. <ul style="list-style-type: none"> ■ Zeichnen Sie die Passphrase auf, die Sie benötigen, um die Datenbank bei einem Ausfall wiederherzustellen oder um nach der Erstinstallation Komponenten hinzuzufügen. ■ Die Passphrase darf keine doppelten Anführungszeichen (") enthalten.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein.

Unternehmensbereitstellungen

Einstellung	Beschreibung
laaS-Web-Adresse	Geben Sie den FQDN des primären laaS-Webserver ein. Wenn Sie eine Unternehmenskonfiguration bereitstellen, die mehrere laaS-Webserver mit Lastausgleich umfasst, geben Sie stattdessen den FQDN des Lastausgleichsdiensts ein.
Manager Service-Adresse	Geben Sie den FQDN des primären Manager Service-Hosts ein. Wenn Sie eine Unternehmenskonfiguration bereitstellen, die mehrere Manager Service-Hosts mit Lastausgleich umfasst, geben Sie stattdessen den FQDN des Lastausgleichsdiensts ein.
Sicherheitskennwortsatz	Erstellen Sie eine Passphrase, um Daten in der laaS-SQL-Datenbank zu verschlüsseln. <ul style="list-style-type: none"> ■ Zeichnen Sie die Passphrase auf, die Sie benötigen, um die Datenbank bei einem Ausfall wiederherzustellen oder um nach der Erstinstallation Komponenten hinzuzufügen. ■ Die Passphrase darf keine doppelten Anführungszeichen (") enthalten.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein.

Microsoft SQL Server

Auf der Seite „Microsoft SQL Server“ konfigurieren Sie die vRealize Automation laaS-SQL-Datenbank. In der laaS-Datenbank werden bereitgestellte Maschinen, zugeordnete Elemente und Richtlinien erfasst.

Einstellung	Beschreibung
Servename	Geben Sie den FQDN des SQL Server-Hosts ein. Dies kann ein laaS-Windows-Server oder ein separater Server sein. Wenn Sie eine Portnummer oder eine benannte Instanz angeben müssen, verwenden Sie das Format FQDN,Port\Instanz. Bei Verwendung von SQL AlwaysOn Availability Group (AAG) geben Sie den AAG-Listener-FQDN an.
Datenbankname	Übernehmen Sie den Standardwert von vra oder geben Sie einen anderen Namen für die laaS-Datenbank ein.
Neue Datenbank erstellen	Erstellen Sie die Datenbank mit dem Installationsassistenten. Damit diese Option funktioniert, muss dem Konto, das den Management-Agent auf dem primären laaS-Webserver ausführt, die sysadmin-Rolle in SQL zugewiesen sein.
Vorhandene leere Datenbank verwenden	Erstellen Sie die Datenbank nicht mit dem Installationsassistenten. Wenn Sie die Datenbank separat erstellen, benötigen die von Ihnen angegebenen Anmeldedaten des Windows- oder SQL-Benutzers die dbo-Berechtigung für die Datenbank.
Standardeinstellungen	(Nur für neue Datenbank) Deaktivieren Sie diese Option nur, wenn Sie einen alternativen Speicherort für laaS-Daten und -Protokolldateien verwenden möchten. Wenn diese Option deaktiviert ist, geben Sie die Verzeichnisse für Daten (MDF) und Protokolle ein. Ihr SQL Server-Dienstkonto benötigt Schreibzugriff auf die Verzeichnisse.
SSL für Datenbankverbindung verwenden	Verschlüsseln Sie die Verbindungen zur Datenbank. Zum Verwenden dieser Option müssen Sie Ihren SQL Server-Host für SSL separat konfigurieren. Darüber hinaus müssen der laaS-Webserver und der Manager Service-Host dem SSL-Zertifikat von Ihrem SQL Server-Host vertrauen.

Einstellung	Beschreibung
Windows-Authentifizierung	<p>Deaktivieren Sie diese Option nur, wenn Sie anstelle der Windows-Authentifizierung die SQL-Authentifizierung verwenden möchten.</p> <p>Wenn diese Option deaktiviert ist, geben Sie Anmeldedaten der SQL-Authentifizierung ein.</p>
Installationspfad	<p>Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein.</p> <ul style="list-style-type: none"> ■ vRealize Automation-Dateien werden nicht auf dem SQL Server-Host installiert. Sie werden auf dem primären IaaS-Webserver platziert. ■ Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.

Webrolle

(Nur Unternehmensbereitstellungen) Auf der Seite „Webrolle“ konfigurieren Sie die vRealize Automation IaaS-Website separat in IIS.

In einer Unternehmensbereitstellung geben Sie die IaaS-Windows-Maschine, die die Webkomponente hostet, separat an. Für Hochverfügbarkeit werden mehrere Hosts unterstützt.

Einstellung	Beschreibung								
Name der Website	<p>Passen Sie den Namen an oder übernehmen Sie die standardmäßige IIS-Website.</p> <p>Sie sollten keine zusätzlichen Websites in IIS hosten. vRealize Automation legt die Bindung des Kommunikationssports für alle nicht zugewiesenen IP-Adressen fest, wodurch keine zusätzlichen Bindungen möglich sind.</p>								
Port	<p>Passen Sie den Port an oder übernehmen Sie den Standardwert 443.</p>								
IaaS-Webserver	<table border="1"> <tr> <td>IaaS-Hostname</td> <td>Geben Sie den FQDN für jede IaaS-Windows-Maschine ein, die die IaaS-Webkomponente hostet.</td> </tr> <tr> <td>Username</td> <td>Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.</td> </tr> <tr> <td>Password</td> <td>Geben Sie das Kennwort des Kontos ein.</td> </tr> <tr> <td>Installationspfad</td> <td> <p>Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein.</p> <p>Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.</p> </td> </tr> </table>	IaaS-Hostname	Geben Sie den FQDN für jede IaaS-Windows-Maschine ein, die die IaaS-Webkomponente hostet.	Username	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.	Password	Geben Sie das Kennwort des Kontos ein.	Installationspfad	<p>Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein.</p> <p>Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.</p>
IaaS-Hostname	Geben Sie den FQDN für jede IaaS-Windows-Maschine ein, die die IaaS-Webkomponente hostet.								
Username	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.								
Password	Geben Sie das Kennwort des Kontos ein.								
Installationspfad	<p>Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein.</p> <p>Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.</p>								

Manager Service-Rolle

(Nur Unternehmensbereitstellungen) Auf der Seite „Manager Service-Rolle“ konfigurieren Sie die separate vRealize Automation-Windows-Maschine, die den IaaS Manager Service hostet.

In einer Unternehmensbereitstellung geben Sie den Host des Manager Service, der ein Windows-Dienst ist, gesondert an. Für Hochverfügbarkeit werden mehrere Hosts unterstützt.

Einstellung	Beschreibung
Active	Wählen Sie den primären Manager Service-Host aus. Zusätzliche Hosts dienen als Sicherungen des primären Hosts. Wenn Sie die Installation mithilfe des Installationsassistenten durchführen, kann ein transparentes Failover des Dienstes auf eine Sicherung durchgeführt werden, wenn ein Problem auftritt. Siehe Informationen zum automatischen Manager Service-Failover .
laaS-Hostname	Geben Sie den FQDN für jede laaS-Windows-Maschine ein, die den Manager Service hostet.
Username	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem laaS Windows-Server sein.
Password	Geben Sie das Kennwort des Kontos ein.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.

Distributed Execution Manager

Auf der Seite „Distributed Execution Manager“ konfigurieren Sie die vRealize Automation-Windows-Maschinen, die laaS-DEMs hosten. Es werden mehrere DEM-Hosts unterstützt.

Einstellung	Beschreibung
laaS-Hostname	Geben Sie den FQDN für jede laaS-Windows-Maschine ein, die einen DEM hostet.
Instanzname	Geben Sie einen eindeutigen Bezeichner für jeden DEM ein. Alle DEM-Namen müssen unabhängig davon, ob sie sich auf demselben oder einem anderen Host befinden, eindeutig sein.
Username	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem laaS Windows-Server sein.
Password	Geben Sie das Kennwort des Kontos ein.
Beschreibung der Instanz	Geben Sie bei Bedarf eine Erläuterung der Workflows ein, die den einzelnen DEMs zugeordnet sind.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.

Agents

Auf der Seite „Agenten“ erstellen Sie die Verknüpfung zwischen vRealize Automation laaS und den Virtualisierungsressourcen, auf denen die Infrastruktur bereitgestellt wird. Sie wählen einen Agent-Typ aus und geben die Details für den entsprechenden Endpoint an.

- Mehrere Agents desselben Typs oder unterschiedlicher Typen werden unterstützt.
- Sie können Agents auf demselben Server oder auf separaten Servern installieren.
- Bei Installation auf demselben Server werden bis zu 25 Agents eines beliebigen Typs unterstützt.

- Wenn sich mehrere Agents desselben Typs auf demselben Server installiert werden, muss jeder von ihnen einen eindeutigen Namen und einen unterschiedlichen Endpoint aufweisen.
- Für Hochverfügbarkeit können Sie einen Agent mit demselben Typ, Namen und Endpoint auf separaten Servern installieren.
- vSphere ist normalerweise einer der Agent-Typen.
- Sie können Agenten nach der Installation hinzufügen.

Agent-Typen

Tabelle 1-20. vSphere

Einstellung	Beschreibung
Agent-Typ	Wählen Sie im Dropdown-Menü vSphere aus.
laaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der laaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Endpoint	Geben Sie einen Namen für den vSphere-Endpoint ein.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem laaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-21. EPI PowerShell

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „EpiPowerShell“ aus.
laaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der laaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Typ	Wählen Sie aus der Dropdown-Liste die Marke der Bereitstellung aus, die der EPI-Server-Endpoint hostet.
Server	Geben Sie den EPIServer-FQDN an.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.

Tabelle 1-21. EPI PowerShell (Fortsetzung)

Einstellung	Beschreibung
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-22. HyperV

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „HyperV“ aus.
IaaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der IaaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Benutzername	Geben Sie das Anmeldekonto für die Instanz des HyperV-Endpoints ein.
Kennwort	Geben Sie das Kennwort des Kontos ein.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-23. VDI PowerShell

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „VdiPowerShell“ aus.
IaaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der IaaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Typ	Der Endpoint-Typ lautet standardmäßig „XenDesktop“ und kann nicht geändert werden.
Server	Geben Sie den FQDN des XenDesktop-Endpoints ein.
XenDesktop-Version	Wählen Sie aus der Dropdown-Liste „Version“ aus.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-24. Xen

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „Xen“ aus.
laaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der laaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Benutzername	Geben Sie das Anmeldekonto für die Instanz des Xen-Endpoints ein.
Kennwort	Geben Sie das Kennwort des Kontos ein.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem laaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-25. WMI

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „WMI“ aus.
laaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der laaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere laaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem laaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

Tabelle 1-26. Testen

Einstellung	Beschreibung
Agent-Typ	Wählen Sie aus der Dropdown-Liste „Test“ aus.
laaS-Hostname	Wählen Sie aus der Dropdown-Liste den FQDN der laaS-Windows-Maschine aus, die den Agent hostet.
Agent-Name	Geben Sie einen eindeutigen Bezeichner ein, es sei denn, Sie fügen denselben Agent-Namen und Endpunkt für Hochverfügbarkeit auf separaten Servern hinzu.

Tabelle 1-26. Testen (Fortsetzung)

Einstellung	Beschreibung
Installationspfad	Lassen Sie dieses Feld leer, um den Standardpfad %ProgramFiles(x86)%\VMware zu übernehmen, oder geben Sie einen alternativen Speicherort ein. Wenn Sie mehrere IaaS-Komponenten auf derselben Windows-Maschine installieren, installieren Sie sie alle in demselben Installationspfad.
Benutzername	Geben Sie das Dienstkonto im Format „DOMAIN\username“ ein. Das Konto muss ein Domänenkonto mit lokalen Administratorrechten auf dem IaaS Windows-Server sein.
Kennwort	Geben Sie das Kennwort des Kontos ein.

vRealize Appliance-Zertifikat

Auf der Seite „vRealize Appliance-Zertifikat“ erstellen Sie das von der vRealize Automation-Appliance verwendete Authentifizierungszertifikat oder wählen es aus. Wenn das Zertifikat selbstsigniert ist, wird es Endbenutzern angezeigt, und sie bestätigen es, wenn sie sich in einem Browser bei vRealize Automation anmelden.

Einstellung	Beschreibung
Zertifikatsaktion	Vorhandene beibehalten Verwenden Sie das Zertifikat, das sich bereits auf dieser vRealize Automation-Appliance befindet. Überprüfen Sie die Details in den Einträgen unten, z. B. die Seriennummer und den Fingerabdruck.
	Zertifikat generieren Verwenden Sie den Assistenten, um ein selbstsigniertes Zertifikat der vRealize Automation-Appliance zu generieren.
Anforderung zur Zertifikats-signierung (CSR) erstellen	Erstellen Sie eine CSR-Datei (Certificate Signing Request, Zertifikatssignieranforderung) für die Zertifizierungsstelle. Eine CSR hilft der Zertifizierungsstelle dabei, ein Zertifikat mit den richtigen Werten zu erstellen, das Sie importieren können. <ol style="list-style-type: none"> Geben Sie die Organisation, die Organisationseinheit und den Ländercode ein (siehe unten). Klicken Sie auf Anforderung zur Zertifikatssignierung (CSR) erstellen. Zum Herunterladen der CSR-Datei für Ihre Zertifizierungsstelle klicken Sie auf den angezeigten Link.
Importieren	Identifizieren Sie eine Zertifikatsdatei im PEM-Format, fügen Sie sie mit dem Assistenten dem richtigen Speicher hinzu und laden Sie sie für die Verwendung durch vRealize Automation. Bei dieser Option werden Sie zur Eingabe des privaten Schlüssels des Zertifikats und des privaten Schlüssels der Passphrase (sofern vorhanden) sowie der Zertifikatskette aufgefordert, es sei denn, Sie importieren ein anhand Ihrer CSR-Datei erstelltes Zertifikat. Wenn Sie eine von einer Zertifizierungsstelle bereitgestellte PEM-Datei importieren, die aus Ihrer CSR-Datei erstellt wurde, lassen Sie die Felder für den privaten Schlüssel und die Passphrase leer.

Einstellung	Beschreibung
Allgemeiner Name	Der FQDN der vRealize Automation-Appliance. In Unternehmensbereitstellungen mit Hochverfügbarkeit und einem Lastausgleichsdienst vor mehreren Appliances handelt es sich bei diesem Eintrag stattdessen um den FQDN des Lastausgleichsdiensts.
Organisation	Geben Sie Ihre größere Abteilung oder Ihren Geschäftsbereich ein.
Organisationseinheit	Geben Sie Ihre kleinere Abteilung oder Ihre Arbeitsgruppe ein.
Landeskennzahl	Geben Sie eine Abkürzung für das Land Ihrer Geschäftstätigkeit ein.
Seriennummer	Eindeutiger alphanumerischer Bezeichner
Fingerabdruck	Eine eindeutige alphanumerische Zeichenfolge zur Identifizierung eines Zertifikats oder zum Vergleich eines Zertifikats mit einem anderen.
Gültig seit	Zeitstempel, nach dem das Zertifikat verwendet werden kann.
Gültig bis	Zeitstempel, nach dem das Zertifikat nicht mehr verwendet werden kann.

Webzertifikat

Auf der Seite „Webzertifikat“ erstellen Sie das vom IaaS-Webserver verwendete Authentifizierungszertifikat oder wählen es aus. Die vRealize Automation-Appliance stellt eine Verbindung zum Webserver her und muss ihn authentifizieren und ihm vertrauen.

Einstellung	Beschreibung
Zertifikatsaktion	<p>Vorhandene beibehalten</p> <p>Zertifikat generieren</p> <p>Anforderung zur Zertifikatssignierung (CSR) erstellen</p>
	<p>Verwenden Sie das Zertifikat, das sich bereits auf diesem IaaS-Webserver befindet. Überprüfen Sie die Details in den Einträgen unten, z. B. die Seriennummer und den Fingerabdruck.</p> <p>Verwenden Sie den Assistenten, um ein selbstsigniertes Zertifikat des IaaS-Webservers zu generieren.</p> <p>Erstellen Sie eine CSR-Datei (Certificate Signing Request, Zertifikatssignieranforderung) für die Zertifizierungsstelle. Eine CSR hilft der Zertifizierungsstelle dabei, ein Zertifikat mit den richtigen Werten zu erstellen, das Sie importieren können.</p> <ol style="list-style-type: none"> Geben Sie die Organisation, die Organisationseinheit und den Ländercode ein (siehe unten). Klicken Sie auf Anforderung zur Zertifikatssignierung (CSR) erstellen. Zum Herunterladen der CSR-Datei für Ihre Zertifizierungsstelle klicken Sie auf den angezeigten Link.

Einstellung	Beschreibung
Importieren	<p>Identifizieren Sie eine Zertifikatsdatei im PEM-Format, fügen Sie sie mit dem Assistenten dem richtigen Speicher hinzu und laden Sie sie für die Verwendung durch vRealize Automation.</p> <p>Bei dieser Option werden Sie zur Eingabe des privaten Schlüssels des Zertifikats und des privaten Schlüssels der Passphrase (sofern vorhanden) sowie der Zertifikatskette aufgefordert, es sei denn, Sie importieren ein anhand Ihrer CSR-Datei erstelltes Zertifikat.</p> <p>Wenn Sie eine von einer Zertifizierungsstelle bereitgestellte PEM-Datei importieren, die aus Ihrer CSR-Datei erstellt wurde, lassen Sie die Felder für den privaten Schlüssel und die Passphrase leer.</p>
Fingerabdruck des Zertifikats bereitstellen	Laden Sie ein Zertifikat, das Sie bereits dem richtigen Speicher hinzugefügt haben.
Allgemeiner Name	<p>Der FQDN des IaaS-Webservers.</p> <p>In Unternehmensbereitstellungen mit Hochverfügbarkeit und einem Lastausgleichsdienst vor mehreren Webservern handelt es sich bei diesem Eintrag stattdessen um den FQDN des Lastausgleichsdiensts.</p>
Organisation	Geben Sie Ihre größere Abteilung oder Ihren Geschäftsbereich ein.
Organisationseinheit	Geben Sie Ihre kleinere Abteilung oder Ihre Arbeitsgruppe ein.
Landeskennzahl	Geben Sie eine Abkürzung für das Land Ihrer Geschäftstätigkeit ein.
Seriennummer	Eindeutiger alphanumerischer Bezeichner
Fingerabdruck	Eine eindeutige alphanumerische Zeichenfolge zur Identifizierung eines Zertifikats oder zum Vergleich eines Zertifikats mit einem anderen.
Gültig seit	Zeitstempel, nach dem das Zertifikat verwendet werden kann.
Gültig bis	Zeitstempel, nach dem das Zertifikat nicht mehr verwendet werden kann.

Manager Service-Zertifikat

(Nur Unternehmensbereitstellungen) Auf der Seite „Manager Service-Zertifikat“ erstellen Sie das vom vRealize Automation IaaS Manager Service-Host verwendete Authentifizierungszertifikat oder wählen es aus. Die anderen IaaS-Windows-Server stellen eine Verbindung zum Manager Service-Host her und müssen ihn authentifizieren und ihm vertrauen.

Diese Seite wird nur angezeigt, wenn Sie den Manager Service auf einer separaten Maschine über den IaaS-Webserver hosten. Wenn sie auf derselben Maschine gehostet werden, stellt das Webzertifikat Authentifizierung für beide Rollen bereit.

Einstellung		Beschreibung
Zertifikatsaktion	Vorhandene beibehalten	Verwenden Sie das Zertifikat, das sich bereits auf diesem IaaS Manager Service-Host befindet. Überprüfen Sie die Details in den Einträgen unten, z. B. die Seriennummer und den Fingerabdruck.
	Zertifikat generieren	Verwenden Sie den Assistenten, um ein selbstsigniertes Zertifikat des IaaS-Manager Service-Hosts zu generieren.
	Anforderung zur Zertifikatsignierung (CSR) erstellen	Erstellen Sie eine CSR-Datei (Certificate Signing Request, Zertifikatssignieranforderung) für die Zertifizierungsstelle. Eine CSR hilft der Zertifizierungsstelle dabei, ein Zertifikat mit den richtigen Werten zu erstellen, das Sie importieren können. <ol style="list-style-type: none"> Geben Sie die Organisation, die Organisationseinheit und den Ländercode ein (siehe unten). Klicken Sie auf Anforderung zur Zertifikatsignierung (CSR) erstellen. Zum Herunterladen der CSR-Datei für Ihre Zertifizierungsstelle klicken Sie auf den angezeigten Link.
	Importieren	Identifizieren Sie eine Zertifikatsdatei im PEM-Format, fügen Sie sie mit dem Assistenten dem richtigen Speicher hinzu und laden Sie sie für die Verwendung durch vRealize Automation. Bei dieser Option werden Sie zur Eingabe des privaten Schlüssels des Zertifikats und des privaten Schlüssels der Passphrase (sofern vorhanden) sowie der Zertifikatskette aufgefordert, es sei denn, Sie importieren ein anhand Ihrer CSR-Datei erstelltes Zertifikat. Wenn Sie eine von einer Zertifizierungsstelle bereitgestellte PEM-Datei importieren, die aus Ihrer CSR-Datei erstellt wurde, lassen Sie die Felder für den privaten Schlüssel und die Passphrase leer.
	Fingerabdruck des Zertifikats bereitstellen	Laden Sie ein Zertifikat, das Sie bereits dem richtigen Speicher hinzugefügt haben.
Allgemeiner Name		Der FQDN des IaaS Manager Service-Hosts. In Unternehmensbereitstellungen mit Hochverfügbarkeit und einem Lastausgleichsdienst vor mehreren Manager Service-Hosts handelt es sich bei diesem Eintrag stattdessen um den FQDN des Lastausgleichsdiensts.
Organisation		Geben Sie Ihre größere Abteilung oder Ihren Geschäftsbereich ein.
Organisationseinheit		Geben Sie Ihre kleinere Abteilung oder Ihre Arbeitsgruppe ein.
Landeskennzahl		Geben Sie eine Abkürzung für das Land Ihrer Geschäftstätigkeit ein.
Seriennummer		Eindeutiger alphanumerischer Bezeichner
Fingerabdruck		Eine eindeutige alphanumerische Zeichenfolge zur Identifizierung eines Zertifikats oder zum Vergleich eines Zertifikats mit einem anderen.

Einstellung	Beschreibung
Gültig seit	Zeitstempel, nach dem das Zertifikat verwendet werden kann.
Gültig bis	Zeitstempel, nach dem das Zertifikat nicht mehr verwendet werden kann.

Lastausgleichsdienste

(Nur Unternehmensbereitstellungen) Auf der Seite „Lastausgleichsmodule“ halten Sie die Konfiguration von Lastausgleichsdiensten für den richtigen Pool von vRealize Automation-Mitgliedssystemen an.

Die Liste der Lastausgleichsdienste dient nur zu Informationszwecken. Basierend auf Ihren früheren Eingaben im Assistenten enthält diese Liste jeden Lastausgleichsdienst in Ihrer Bereitstellung zusammen mit den Mitgliedern, der Komponentenrolle, dem FQDN und der Portnummer.

Ziehen Sie die Liste zurate, während Sie sich bei Ihren Lastausgleichsdiensten anmelden, um vRealize Automation-Mitglieder hinzuzufügen und Ports zu öffnen.

Validierung

Auf der Seite „Validierung“ stellen Sie sicher, dass die vRealize Automation-Installation fortgesetzt werden kann.

Um zu überprüfen, ob alle vRealize Automation-Komponenten, -Rollen und -Konten korrekt sind und ob sich die Systeme gegenseitig authentifizieren können, klicken Sie auf **Validieren**. Je nach Ihrer Umgebung kann der Prozess bis zu einer halben Stunde oder mehr dauern.

Wenn Fehler auftreten, erweitern Sie die fehlerhafte Position und nehmen Sie basierend auf den angegebenen Status und Meldungen Korrekturen vor. Die vRealize Automation-Installation kann erst fortgesetzt werden, nachdem die Validierung erfolgreich abgeschlossen wurde.

Snapshots erstellen

Auf der Seite „Snapshots erstellen“ erstellen Sie VM-Snapshots von allen vRealize Automation-Komponenten, bevor Sie mit der Installation fortfahren.

Auch wenn die Validierung bestanden wurde, sollten Sie unbedingt auf unerwartete Installationsprobleme vorbereitet sein. Verwenden Sie vor Installationsbeginn Ihren vSphere-Client, um einen Snapshot von jeder vRealize Automation-Appliance und jedem IaaS-Windows-Server zu erstellen. Andernfalls müssen Sie alle Assistenteneinstellungen erneut eingeben, um zu diesem Punkt zurückzukehren.

Wenn Sie über ausreichend Ressourcen verfügen, können Sie Snapshots von virtuellen Maschinen erstellen, die ausgeführt werden. Es ist jedoch besser, diese zunächst zu beenden.

- 1 Klicken Sie oben rechts im Installationsassistenten auf **Abmelden**.

Wichtig Wenn Sie den Assistenten nicht über **Abmelden** schließen, sondern auf anderem Weg, können Sie ihn nicht erneut öffnen.

- 2 Fahren Sie in vSphere das Gastbetriebssystem aller vRealize Automation-Appliances und IaaS-Windows-Server herunter.

- 3 Klicken Sie mit der rechten Maustaste auf die virtuellen Maschinen und wählen Sie **Snapshot erstellen** aus.
- 4 Benennen Sie den Snapshot.
- 5 Wenn Sie den Maschinenarbeitspeicher in den Snapshot aufnehmen möchten, wählen Sie **Snapshot des Arbeitsspeichers der virtuellen Maschine** aus.
- 6 Klicken Sie auf **OK**.
Warten Sie, bis die Snapshots erstellt werden.
- 7 Schalten Sie das Gastbetriebssystem aller vRealize Automation-Appliances und IaaS-Windows-Server ein.
- 8 Kehren Sie zur Snapshot-Seite des Installationsassistenten zurück, indem Sie sich erneut als Root-Benutzer anmelden.
<https://vrealize-automation-appliance-FQDN:5480>

Installationsdetails

Auf der Seite „Installationsdetails“ starten Sie die vRealize Automation-Installation oder wiederholen sie, falls Probleme aufgetreten sind.

Klicken Sie zum Starten der Installation auf **Installieren**. Abhängig von Ihrer Umgebung kann die Installation länger als eine Stunde dauern.

Während oder nach der Installation können Sie auf die Schaltfläche **Protokolle erfassen** klicken.

- Wenn Sie Protokolle erfassen, wird oberhalb der Statustabelle ein Link für den Download einer ZIP-Datei angezeigt.
- Wenn Sie mehr als einmal Protokolle erfassen, überschreibt jede neue Erfassung die vorherige.

Wenn Sie die aktuellen Protokolle benötigen, laden Sie sie herunter, bevor Sie erneut auf **Protokolle erfassen** klicken.

Bei Problemen hält der Assistent die Installation an und zeigt Meldungen an, die Sie bei den Korrekturen unterstützen. Nach dem Auswerten der Meldungen und dem Notieren der erforderlichen Korrekturen benötigen Sie möglicherweise die erstellten Snapshots.

Snapshots nicht wiederherstellen

Wenn der Assistent **Wiederholung fehlgeschlagen** aktiviert, nehmen Sie die Korrekturen vor und wiederholen die Installation, ohne Snapshots von Maschinen wiederherzustellen.

Klicken Sie nach den Korrekturen auf **Wiederholung fehlgeschlagen**.

Snapshots von IaaS -Windows-Servern wiederherstellen

Wenn der Assistent **Alle IaaS wiederholen** aktiviert, führen Sie die folgenden Schritte aus.

- 1 In vSphere stellen Sie die Snapshots aller IaaS-Windows-Maschinen wieder her, die auf der vorherigen Assistentenseite erstellt wurden.

- 2 Wenn die Snapshots nach dem Herunterfahren erstellt wurden, schalten Sie die Gastbetriebssysteme ein.
- 3 Wenn Sie einen externen SQL Server-Computer verwendet haben, löschen Sie die vRealize Automation-SQL-Datenbank.
- 4 Nehmen Sie die Korrekturen vor.
- 5 Klicken Sie auf **Alle IaaS wiederholen**.

Snapshots von Appliances und IaaS -Windows-Servern wiederherstellen

Wenn der Assistent Meldungen zu der vRealize Automation-Appliance anzeigt, führen Sie die folgenden Schritte aus.

- 1 Stellen Sie in vSphere die auf der vorherigen Assistentenseite erstellten Snapshots aller vRealize Automation-Appliances und IaaS-Windows-Maschinen wieder her.
- 2 Wenn die Snapshots nach dem Herunterfahren erstellt wurden, schalten Sie die Gastbetriebssysteme ein.
- 3 Wenn Sie einen externen SQL Server-Computer verwendet haben, löschen Sie die vRealize Automation-SQL-Datenbank.
- 4 Nehmen Sie die Korrekturen vor.
- 5 Kehren Sie zum Installationsassistenten zurück, indem Sie sich erneut als Root-Benutzer anmelden.
<https://vrealize-automation-appliance-FQDN:5480>
- 6 Kehren Sie zur Seite „Installationsdetails“ zurück und klicken Sie auf **Installieren**.

Lizenzierung

Auf der Seite „Lizenzierung“ geben Sie einen Schlüssel ein, um das installierte vRealize Automation-Produkt zu aktivieren.

Geben Sie unter **Neuer Lizenzschlüssel** Ihren Schlüssel ein und klicken Sie auf **Schlüssel senden**. Sie können mehr als einen Schlüssel separat senden, einschließlich der Schlüssel für eigenständige vRealize Automation-, vRealize Suite-, vRealize Business for Cloud- und vRealize Code Stream-Instanzen.

Auf dieser Seite wählen Sie auch aus, ob vRealize Code Stream aktiviert wird. vRealize Code Stream wird für Hochverfügbarkeits- oder Produktionsbereitstellungen von vRealize Automation nicht unterstützt und erfordert das vRealize Code Stream Management Pack. Weitere Informationen finden Sie unter [Lizenzierung von vRealize Code Stream](#).

Telemetrie

Auf der Seite „Telemetrie“ entscheiden Sie, ob vRealize Automation im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit Nutzungsstatistiken an VMware sendet.

Aktivieren oder deaktivieren Sie die Option zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP).

Weitere Informationen finden Sie unter [Programm zur Verbesserung der Benutzerfreundlichkeit](#).

Optionen nach der Installation

Auf der Seite „Optionen nach der Installation“ stehen Optionen zum Erstellen neuer vRealize Automation-Daten oder Migrieren älterer Bereitstellungsdaten auf die neue Installation zur Verfügung.

- **Anfängliche Inhalte konfigurieren** erstellt einen neuen lokalen Benutzer des Standardmandanten. Dieser lokale Benutzer kann den Konfigurationsvorgang im Standardmandanten beginnen.
Für diese Option müssen Sie zuvor auf der Seite „Agenten“ des Installationsassistenten mindestens einen vSphere-Endpoint hinzugefügt haben.
- **Eine Bereitstellung migrieren** überträgt Ihre älteren vRealize Automation-Daten an diese neu installierte Bereitstellung. Bei der Migration werden grundlegende Elemente wie Gruppen, Blueprints und Endpoints beibehalten.
- Über **Fortfahren** gelangen Sie zum Ende des Installationsassistenten.

Konfiguration von anfänglichen Inhalten

Auf der Seite „Konfiguration von anfänglichen Inhalten“ erstellen Sie einen neuen lokalen vRealize Automation-Standardmandantenbenutzer, der einen Inhaltsworkflow für einen vSphere-Endpoint beginnen kann.

Hinweis Diese Option ist nur verfügbar, wenn Sie zuvor auf der Seite „Agenten“ mindestens einen vSphere-Endpoint hinzugefügt haben.

Der neue lokale Benutzername ist „configurationadmin“. vRealize Automation gewährt „configurationadmin“ die folgenden Berechtigungen.

- Mandantenadministrator
- IaaS-Administrator
- Genehmigungsadministrator
- Katalog-Administrator
- Infrastrukturarchitekt
- XaaS-Architekt
- vRealize Orchestrator-Administrator

Geben Sie ein Kennwort für „configurationadmin“ ein und bestätigen Sie es. Klicken Sie auf **Anfängliche Inhalte erstellen**, um ein Katalogelement zu generieren, sodass „configurationadmin“ den Konfigurationsvorgang nach der Anmeldung beim Standardmandanten starten kann.

Migrationskonfiguration

Auf der Seite „Migrationskonfiguration“ können Sie die Übertragung von einer anderen, älteren vRealize Automation-Bereitstellung an die neu installierte Bereitstellung starten.

Gehen Sie vor dem Migrieren einer älteren Bereitstellung die folgenden Richtlinien durch.

- Überprüfen Sie das vRealize Automation-Migrationshandbuch der älteren Bereitstellungsversion sorgfältig. Voraussetzungen und andere Details können variieren.

- Migrieren Sie die älteren Mandanten und Identitätsquellen auf VMware Identity Manager in der neuen Bereitstellung.
- Klonen Sie die ältere IaaS SQL Server-Datenbank und stellen Sie sie in der IaaS-Datenbank der neuen Bereitstellung wieder her. Notieren Sie den Namen der geklonten Datenbank.
- Rufen Sie den Verschlüsselungsschlüssel für die ältere IaaS SQL Server-Datenbank ab und notieren Sie ihn.
- Erstellen Sie eine neue Passphrase zum erneuten Verschlüsseln der migrierten Daten und notieren Sie sie.
- Notieren Sie den FQDN der älteren vRealize Automation-Appliance oder des Lastausgleichsdiensts sowie die Root-Anmeldedaten.
- Notieren Sie die Root-Anmeldedaten der neuen Bereitstellung.

Die vRealize Automation -Standard-Installationsschnittstellen

Nachdem der Installationsassistent ausgeführt wurde, müssen oder möchten Sie möglicherweise bestimmte Installationsaufgaben manuell über die Standardschnittstellen durchführen.

Der unter [Installieren von vRealize Automation mit dem Installationsassistenten](#) beschriebene Installationsassistent ist Ihr primäres Tool für neue Installationen von vRealize Automation. Nachdem der Assistent ausgeführt wurde, müssen einige Vorgänge weiterhin im Rahmen des älteren manuellen Installationsvorgangs durchgeführt werden.

Sie müssen die manuellen Schritte durchführen, wenn Sie eine vRealize Automation-Bereitstellung erweitern möchten oder wenn der Assistent aus einem beliebigen Grund beendet wurde. Die Verfahren in diesem Abschnitt müssen möglicherweise in den folgenden Situationen durchgeführt werden.

- Sie haben den Assistenten vor Abschluss der Installation abgebrochen.
- Die Installation über den Assistenten ist fehlgeschlagen.
- Sie möchten eine weitere vRealize Automation-Appliance für Hochverfügbarkeit hinzufügen.
- Sie möchten einen weiteren IaaS-Webserver für Hochverfügbarkeit hinzufügen.
- Sie benötigen einen anderen Proxy-Agent.
- Sie benötigen einen anderen DEM-Worker oder -Orchestrator.

Sie können alle oder nur einige der manuellen Verfahren nutzen. Sehen Sie die Informationen im gesamten Abschnitt durch und verwenden Sie dann die Verfahren, die für Ihre Situation geeignet sind.

Verwenden der Standardschnittstellen für minimale Bereitstellungen

Sie können eine eigenständige Minimalbereitstellung für die Verwendung in einer Entwicklungsumgebung oder als eine Prüfung des Konzepts installieren. Minimalbereitstellungen sind für eine Produktionsumgebung nicht geeignet.

Checkliste für Minimalbereitstellung

Sie installieren vRealize Automation in einer Minimalkonfiguration für die Arbeit in einer Proof-of-Concept- oder Entwicklungsumgebung. Für Minimalbereitstellungen sind weniger Installationsschritte erforderlich. Es steht jedoch nicht die Produktionskapazität einer Unternehmensbereitstellung zur Verfügung.

Führen Sie die allgemeinen Aufgaben in der folgenden Reihenfolge durch.

Tabelle 1-27. Checkliste für Minimalbereitstellung

	Aufgabe	Details
<input type="checkbox"/>	Planen Sie die Umgebung und sorgen Sie dafür, dass die Installationsvoraussetzungen erfüllt sind.	Vorbereitung für die Installation von vRealize Automation
<input type="checkbox"/>	Erstellen Sie eine nicht konfigurierte vRealize Automation-Appliance.	Bereitstellen der vRealize Automation-Appliance
<input type="checkbox"/>	Führen Sie die manuelle Konfiguration der vRealize Automation-Appliance durch.	Konfigurieren der vRealize Automation-Appliance
<input type="checkbox"/>	Installieren Sie IaaS-Komponenten auf einem einzelnen Windows Server.	Installieren der IaaS-Komponenten
<input type="checkbox"/>	Installieren Sie zusätzliche Agents, falls erforderlich.	Installieren der vRealize Automation-Agents
<input type="checkbox"/>	Führen Sie Aufgaben nach der Installation aus, wie beispielsweise das Konfigurieren des Standardmandanten.	Konfigurieren des Zugriffs auf den Standardmandanten

Konfigurieren der vRealize Automation -Appliance

Die vRealize Automation-Appliance ist eine teilweise konfigurierte virtuelle Maschine, die den Server und das Benutzer-Webportal von vRealize Automation hostet. Sie laden die Vorlage für das Open Virtualization Format (OVF) der Appliance auf vCenter Server oder die ESX/ESXi-Inventarliste herunter und stellen sie bereit.

Voraussetzungen

- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).
- Rufen Sie ein Authentifizierungszertifikat für die vRealize Automation-Appliance ab.

Verfahren

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

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

Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.

- 2 Wenn der Installationsassistent angezeigt wird, beenden Sie ihn, damit Sie anstelle des Assistenten zur Verwaltungsschnittstelle wechseln können.

- 3 Wählen Sie **Admin > Uhrzeiteinstellungen** aus und legen Sie die Quelle für die Uhrzeitsynchronisierung fest.

Option	Beschreibung
Hostuhrzeit	Mit ESXi-Host der vRealize Automation-Appliance synchronisieren.
Zeitserver	Mit externem Network Time Protocol (NTP)-Server synchronisieren. Geben Sie den FQDN oder die IP-Adresse des NTP-Servers ein.

Sie müssen die vRealize Automation-Appliances und IaaS-Windows-Server mit derselben Zeitquelle synchronisieren. Verwenden Sie innerhalb einer vRealize Automation-Bereitstellung niemals verschiedene Zeitquellen.

- 4 Wählen Sie **vRA-Einstellungen > Hosteinstellungen** aus.

Option	Aktion
Automatisch lösen	Wählen Sie Automatisch lösen aus, um den Namen des aktuellen Hosts für die vRealize Automation-Appliance anzugeben.
Host aktualisieren	<p>Wählen Sie für neue Hosts die Option Host aktualisieren aus. Geben Sie den vollqualifizierten Domännennamen der vRealize Automation-Appliance, <i>vra-hostname.domain.name</i>, in das Textfeld Hostname ein.</p> <p>Wählen Sie für verteilte Bereitstellungen mit Lastausgleichsdiensten die Option Host aktualisieren aus. Geben Sie den vollqualifizierten Domännennamen für den Lastausgleichsserver, <i>vra-loadbalancename.domain.name</i>, in das Textfeld Hostname ein.</p>

Hinweis Konfigurieren Sie SSO-Einstellungen gemäß der Beschreibung weiter unten in diesem Verfahren immer dann, wenn Sie **Host aktualisieren** zum Festlegen des Hostnamens verwenden.

- 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.

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

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

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

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

Option	Aktion
Anforderung zur Zertifikatssignierung (CSR) erstellen	<p>a Wählen Sie Anforderung zur Zertifikatssignierung (CSR) erstellen aus.</p> <p>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.</p> <p>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.</p> <p>d Wenn Sie das vorbereitete Zertifikat erhalten, klicken Sie auf Import und befolgen Sie die Anweisungen zum Importieren eines Zertifikats in vRealize Automation.</p>
Importieren	<p>a Kopieren Sie die Zertifikatwerte von BEGIN PRIVATE KEY zu END PRIVATE KEY, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld RSA-Privatschlüssel ein.</p> <p>b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld Zertifikatskette ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu.</p> <p>Hinweis Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</p> <p>c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld Passphrase ein.</p>

- 6 Klicken Sie auf **Einstellungen speichern**, um Hostinformationen und SSL-Konfiguration zu speichern.
- 7 Konfigurieren Sie die SSO-Einstellungen.
- 8 Klicken Sie auf **Messaging**. Die Konfigurationseinstellungen und der Status des Messaging für Ihre Appliance werden angezeigt. Ändern Sie diese Einstellungen nicht.
- 9 Klicken Sie auf die Registerkarte **Telemetrie**, um auszuwählen, ob Sie am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program, CEIP) von VMware teilnehmen möchten.

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>.

- Aktivieren Sie **Join the VMware Customer Experience Improvement Program**, um an diesem Programm teilzunehmen.
- Deaktivieren Sie **Join the VMware Customer Experience Improvement Program**, um nicht an diesem Programm teilzunehmen.

- 10 Klicken Sie auf **Services** und stellen Sie sicher, dass Dienste registriert sind.

Je nach Site-Konfiguration kann dies etwa 10 Minuten dauern.

Hinweis Sie können sich bei der Appliance anmelden und `tail -f /var/log/vcac/catalina.out` ausführen, um das Starten der Dienste zu überwachen.

- 11 Geben Sie Ihre Lizenzinformationen ein.

- a Klicken Sie auf **vRA-Einstellungen > Lizenzierung**.
- b Klicken Sie auf **Lizenzierung**.
- c Geben Sie einen gültigen vRealize Automation-Lizenzschlüssel ein, den Sie beim Herunterladen der Installationsdateien heruntergeladen haben, und klicken Sie auf **Schlüssel senden**.

Hinweis Wenn ein Verbindungsfehler auftritt, liegt möglicherweise ein Problem mit dem Lastausgleichsdienst vor. Überprüfen Sie die Netzwerkkonnektivität zum Lastausgleichsdienst.

- 12 Wählen Sie, ob vRealize Code Stream aktiviert werden soll, und geben Sie eine vRealize Code Stream-Lizenz ein.

vRealize Code Stream wird für Hochverfügbarkeits- oder Produktionsbereitstellungen von vRealize Automation nicht unterstützt.

- 13 Überprüfen Sie, ob Sie sich bei vRealize Automation anmelden können.

- a Öffnen Sie die URL für die vRealize Automation-Produktschnittstelle in einem Webbrowser.
`https://vrealize-automation-appliance-FQDN/vcac`
- b Akzeptieren Sie das vRealize Automation-Zertifikat.
- c Akzeptieren Sie das SSO-Zertifikat.
- d Melden Sie sich mit `administrator@vsphere.local` und dem Kennwort an, das Sie bei der Konfiguration von SSO angegeben haben.

Die Schnittstelle wird mit der Seite „Mandanten“ auf der Registerkarte **Administration** geöffnet. Ein einzelner Mandant mit dem Namen `vsphere.local` wird in der Liste angezeigt.

Sie haben die Bereitstellung und Konfiguration Ihrer vRealize Automation-Appliance abgeschlossen. Wenn die Appliance nach der Konfiguration nicht ordnungsgemäß funktioniert, stellen Sie die Appliance erneut bereit und konfigurieren Sie sie neu. Nehmen Sie bei der vorhandenen Appliance keine Änderungen vor.

Nächste Schritte

Siehe [Installieren der Infrastrukturkomponenten](#).

Installieren der IaaS-Komponenten

Der Administrator installiert einen kompletten Satz an Infrastrukturkomponenten (IaaS) auf einer Windows-Maschine (physisch oder virtuell). Zum Ausführen dieser Aufgaben sind Administratorrechte erforderlich.

Bei einer Minimalinstallation werden alle Komponenten auf demselben Windows-Server installiert, mit Ausnahme der SQL-Datenbank, die Sie auf einem separaten Server installieren können.

Aktivieren der Zeitsynchronisierung auf dem Windows-Server

Die Uhren auf dem vRealize Automation-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Die folgenden Schritte beschreiben, wie Sie mithilfe von VMware Tools die Zeitsynchronisierung für den ESX/ESXi-Host aktivieren. Wenn Sie die IaaS-Komponenten auf einem physischen Host installieren oder VMware Tools nicht für die Zeitsynchronisierung verwenden möchten, stellen Sie mithilfe Ihrer bevorzugten Methode sicher, dass die Serveruhrzeit stimmt.

Verfahren

- 1 Öffnen Sie auf der Windows-Installationsmaschine eine Eingabeaufforderung.
- 2 Geben Sie den folgenden Befehl ein, um zum Verzeichnis „VMware Tools“ zu navigieren.

```
cd C:\Programme\VMware\VMware Tools
```

- 3 Geben Sie den Befehl zum Anzeigen des Zeitsynchronisierungsstatus ein.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Wenn die Zeitsynchronisierung deaktiviert ist, geben Sie den folgenden Befehl zum Aktivieren der Zeitsynchronisierung ein.

```
VMwareToolboxCmd.exe timesync enable
```

IaaS-Zertifikate

vRealize Automation-IaaS-Komponenten verwenden Zertifikate und SSL für die sichere Kommunikation zwischen Komponenten. Bei einer Minimalinstallation für eine Machbarkeitsstudie können Sie selbstsignierte Zertifikate verwenden.

Beziehen Sie in einer verteilten Umgebung ein Domänenzertifikat von einer vertrauenswürdigen Zertifizierungsstelle. Informationen zum Installieren von Domänenzertifikaten für IaaS-Komponenten finden Sie unter [Installieren der IaaS-Zertifikate](#) im Kapitel zu verteilten Bereitstellungen.

Installieren der Infrastrukturkomponenten

Der Systemadministrator meldet sich bei der Windows-Maschine an und folgt dem Installationsassistenten zum Installieren der IaaS-Dienste auf der virtuellen oder physischen Windows-Maschine.

Voraussetzungen

- Stellen Sie sicher, dass der Server die unter [IaaS-Windows-Server](#) erläuterten Anforderungen erfüllt.
- [Aktivieren der Zeitsynchronisierung auf dem Windows-Server](#).
- Stellen Sie sicher, dass Sie die vRealize Automation-Appliance bereitgestellt und vollständig konfiguriert haben, und dass die notwendigen Dienste ausgeführt werden (Plug-In-Dienst, Katalogdienst, IaaS-Proxy-Anbieter).

Verfahren

1 [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#)

Für die Installation von IaaS auf einem minimalen virtuellen oder physischen Windows-Server laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

2 [Auswählen des Installationstyps](#)

Der Systemadministrator führt den Installationsassistenten über die Installationsmaschine mit Windows 2008 oder 2012 aus.

3 [Prüfen der Voraussetzungen](#)

Die Voraussetzungsprüfung stellt sicher, dass Ihre Maschine IaaS-Installationsanforderungen erfüllt.

4 [Angaben der Servers und Kontoeinstellungen](#)

Der vRealize Automation-Systemadministrator legt Server- und Kontoeinstellungen für den Windows-Installationsserver fest und wählt eine SQL-Datenbank-Server-Instanz sowie eine Authentifizierungsmethode aus.

5 [Angaben von Managern und Agents](#)

Bei der Minimalinstallation werden die erforderlichen Distributed Execution Managers und der vSphere-Standard-Proxy-Agent installiert. Der Systemadministrator kann nach der Installation mithilfe des benutzerdefinierten Installationsprogramms zusätzliche Proxy-Agents installieren (z. B. Xen-Server oder Hyper-V).

6 [Registrieren der IaaS-Komponenten](#)

Der Systemadministrator installiert das IaaS-Zertifikat und registriert die IaaS-Komponenten mit SSO.

7 [Abschließen der Installation](#)

Der Systemadministrator schließt die IaaS-Installation ab.

Herunterladen des Installationsprogramms für vRealize Automation IaaS

Für die Installation von IaaS auf einem minimalen virtuellen oder physischen Windows-Server laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

Voraussetzungen

- Überprüfen Sie die IaaS-Windows-Serveranforderungen. Siehe [IaaS-Windows-Server](#).
- Achten Sie bei Verwendung von Internet Explorer zum Herunterladen darauf, dass „Verstärkte Sicherheitskonfiguration“ nicht aktiviert ist. Navigieren Sie auf dem Windows-Server zu `res://iesetup.dll/SoftAdmin.htm`.

Verfahren

- 1 Melden Sie sich auf dem IaaS-Windows-Server mit einem Konto mit Administratorrechten an.
- 2 Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance direkt in einem Webbrowser.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Klicken Sie auf **IaaS-Installationsprogramm**.
- 4 Speichern Sie `setup__vrealize-automation-appliance-FQDN@5480` auf dem Windows-Server.
Ändern Sie den Dateinamen des Installationsprogramms nicht. Er wird verwendet, um die Installation mit der vRealize Automation-Appliance zu verbinden.

Auswählen des Installationstyps

Der Systemadministrator führt den Installationsassistenten über die Installationsmaschine mit Windows 2008 oder 2012 aus.

Voraussetzungen

[Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.
 - a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.
Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
 - b Wählen Sie **Zertifikat akzeptieren** aus.
 - c Klicken Sie auf **Zertifikat anzeigen**.
Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

- 5 Wählen Sie **Zertifikat akzeptieren** aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie die Option **Installation abschließen** auf der Seite **Installationstyp** aus, wenn Sie eine minimale Bereitstellung erstellen, und klicken Sie auf **Weiter**.

Prüfen der Voraussetzungen

Die Voraussetzungsprüfung stellt sicher, dass Ihre Maschine IaaS-Installationsanforderungen erfüllt.

Voraussetzungen

[Auswählen des Installationstyps.](#)

Verfahren

- 1 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
Keine Fehler	Klicken Sie auf Weiter .
Nicht kritische Fehler	Klicken Sie auf Umgehung .
Kritische Fehler	Durch Umgehen kritischer Fehler schlägt die Installation fehl. Wenn Warnungen angezeigt werden, wählen Sie die Warnung im linken Fensterbereich aus und folgen Sie den Anleitungen im rechten Bereich. Behandeln Sie alle kritischen Fehler und klicken Sie zum Überprüfen auf Erneut prüfen .

- 2 Klicken Sie auf **Weiter**.

Die Maschine erfüllt die Installationsanforderungen.

Angeben der Servers und Kontoeinstellungen

Der vRealize Automation-Systemadministrator legt Server- und Kontoeinstellungen für den Windows-Installationsserver fest und wählt eine SQL-Datenbank-Server-Instanz sowie eine Authentifizierungsmethode aus.

Voraussetzungen

[Prüfen der Voraussetzungen.](#)

Verfahren

- 1 Geben Sie auf der Seite **Server- und Kontoeinstellungen** oder der Seite **Erkannte Einstellungen** den Benutzernamen und das Kennwort für das Windows-Dienstkonto ein. Dieses Dienstkonto muss ein lokales Administratorkonto sein, das auch über administrative SQL-Berechtigungen verfügt.

- 2 Geben Sie im Textfeld **Kennwortsatz** einen Satz ein.

Bei einem Kennwortsatz handelt es sich um eine Reihe von Wörtern zur Generierung des Verschlüsselungsschlüssels, welcher zum Schutz der Daten in der Datenbank verwendet wird.

Hinweis Speichern Sie Ihren Kennwortsatz, sodass er für zukünftige Installationen oder Systemwiederherstellungen verfügbar ist.

- 3 Um die Datenbankinstanz auf demselben Server mit den IaaS-Komponenten zu installieren, akzeptieren Sie den Standardserver im Textfeld **Server** im Abschnitt mit den Installationsinformationen für die SQL Server-Datenbank.

Wenn sich die Datenbank auf einer anderen Maschine befindet, geben Sie den Server im folgenden Format ein.

Maschinen-FQDN,Portnummer\benannte-Datenbank-Instanz

- 4 Akzeptieren Sie im Textfeld **Datenbankname** den Standardnamen oder geben Sie gegebenenfalls einen entsprechenden Namen ein.

- 5 Wählen Sie die Authentifizierungsmethode aus.

- ◆ Wählen Sie **Windows-Authentifizierung verwenden** aus, wenn Sie eine Datenbank mit den Windows-Anmeldedaten des aktuellen Benutzers erstellen möchten. Der Benutzer muss über SQL-Systemadministratorrechte verfügen.
- ◆ Deaktivieren Sie **Windows-Authentifizierung verwenden**, wenn Sie eine Datenbank mit SQL-Authentifizierung erstellen möchten. Geben Sie den **Benutzernamen** und das **Kennwort** des SQL Server-Benutzers ein, der über SQL-Systemadministratorrechte auf der SQL Server-Instanz verfügt.

Die Windows-Authentifizierung wird empfohlen. Wenn Sie die SQL-Authentifizierung auswählen, wird das Kennwort für die unverschlüsselte Datenbank in bestimmten Konfigurationsdateien angezeigt.

- 6 (Optional) Aktivieren Sie das Kontrollkästchen **SSL für Datenbankverbindung verwenden**.

Dieses Kontrollkästchen ist standardmäßig aktiviert. SSL ermöglicht eine sicherere Verbindung zwischen dem IaaS-Server und der SQL-Datenbank. Sie müssen jedoch zunächst SSL auf dem SQL Server konfigurieren, damit diese Option unterstützt wird. Weitere Informationen zum Konfigurieren von SSL auf dem SQL-Server finden Sie im [Microsoft Technet-Artikel 189067](#).

- 7 Klicken Sie auf **Weiter**.

Angeben von Managern und Agents

Bei der Minimalinstallation werden die erforderlichen Distributed Execution Managers und der vSphere-Standard-Proxy-Agent installiert. Der Systemadministrator kann nach der Installation mithilfe des benutzerdefinierten Installationsprogramms zusätzliche Proxy-Agents installieren (z. B. XenServer oder Hyper-V).

Voraussetzungen

[Angeben der Servers und Kontoeinstellungen](#).

Verfahren

- 1 Akzeptieren Sie auf der Seite **Distributed Execution Managers And Proxy vSphere Agent** die Standardeinstellungen oder ändern Sie die Namen gegebenenfalls.
- 2 Akzeptieren Sie für die Installation eines vSphere-Agent die Standardeinstellungen, um die Bereitstellung mit vSphere zu aktivieren, oder deaktivieren Sie es gegebenenfalls.
 - a Wählen Sie **vSphere-Agent installieren und konfigurieren** aus.
 - b Akzeptieren Sie den Standard-Agent und -Endpoint oder geben Sie einen Namen ein.

Notieren Sie sich den Wert des Endpoint-Namens. Sie müssen diese Informationen korrekt eingeben, wenn Sie den vSphere-Endpoint in der vRealize Automation-Konsole konfigurieren. Andernfalls schlägt die Konfiguration möglicherweise fehl.
- 3 Klicken Sie auf **Weiter**.

Registrieren der IaaS-Komponenten

Der Systemadministrator installiert das IaaS-Zertifikat und registriert die IaaS-Komponenten mit SSO.

Voraussetzungen

[Herunterladen des Installationsprogramms für vRealize Automation IaaS.](#)

Verfahren

- 1 Akzeptieren Sie den **Server**-Standardwert, der mit dem vollqualifizierten Domännennamen des vRealize Automation-Appliance-Servers aufgefüllt wird, von dem Sie das Installationsprogramm heruntergeladen haben. Stellen Sie sicher, dass ein vollqualifizierter Domänenname zur Identifizierung des Servers und nicht einer IP-Adresse verwendet wird.

Wenn Sie über mehrere virtuelle Appliances verfügen und einen Lastausgleichsdienst verwenden, geben Sie den Pfad der virtuellen Appliance des Lastausgleichsdiensts ein.
- 2 Klicken Sie auf **Laden**, um den Wert für **SSO-Standardmandant** (vsphere.local) auszufüllen.
- 3 Klicken Sie auf **Herunterladen**, um das Zertifikat aus der vRealize Automation-Appliance herunterzuladen.

Zum Anzeigen der Zertifikatsdetails können Sie auf **Zertifikat anzeigen** klicken.
- 4 Wählen Sie **Zertifikat akzeptieren** aus, um das SSO-Zertifikat zu installieren.
- 5 Geben Sie im Feld für den SSO-Administrator **Administrator** in das Textfeld **Benutzername** und das Kennwort ein, das Sie für diesen Benutzer beim Konfigurieren von SSO in **Kennwort** und **Kennwort bestätigen** festgelegt haben.
- 6 Klicken Sie auf den Testlink rechts vom Feld **Benutzername**, um das eingegebene Kennwort zu überprüfen.
- 7 Akzeptieren Sie den Standardwert in **IaaS-Server**, der den Hostnamen der Windows-Maschine enthält, auf der Sie die Installation durchführen.
- 8 Klicken Sie auf den Testlink rechts vom Feld **IaaS-Server**, um die Konnektivität zu überprüfen.

9 Klicken Sie auf **Weiter**.

Wenn Sie auf **Weiter** klicken und es wird daraufhin ein Fehler angezeigt, beheben Sie diesen, bevor Sie den Vorgang fortsetzen.

Abschließen der Installation

Der Systemadministrator schließt die IaaS-Installation ab.

Voraussetzungen

- [Registrieren der IaaS-Komponenten](#).
- Stellen Sie sicher, dass die Maschine, auf der Sie installieren, mit dem Netzwerk verbunden ist und eine Verbindung mit der vRealize Automation-Appliance herstellen kann, von der Sie das IaaS-Installationsprogramm herunterladen.

Verfahren

- 1 Überprüfen Sie die Informationen auf der Seite **Bereit zur Installation** und klicken Sie auf **Installieren**.

Die Installation wird gestartet. In Abhängigkeit von Ihrer Netzwerkkonfiguration kann die Installation zwischen fünf Minuten und einer Stunde dauern.

- 2 Wenn die Erfolgsmeldung angezeigt wird, lassen Sie das Kontrollkästchen **Anweisungen für Erstkonfiguration** aktiviert und klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
- 3 Schließen Sie das Meldungsfeld **System konfigurieren**.

Die Installation ist damit abgeschlossen.

Nächste Schritte

[Überprüfen der IaaS-Services](#).

Verwenden der Standardschnittstellen für verteilte Bereitstellungen

Unternehmensbereitstellungen sind für höhere vRealize Automation-Kapazität in der Produktion vorgesehen und erfordern, dass Sie die Komponenten auf mehrere Maschinen verteilen. Unternehmensbereitstellungen können auch redundante Systeme hinter Lastausgleichsdiensten enthalten.

Checkliste für die verteilte Bereitstellung

Ein Systemadministrator kann vRealize Automation in einer verteilten Konfiguration bereitstellen, die Failover-Schutz und High Availability durch Redundanz bietet.

Die Checkliste für die verteilte Bereitstellung liefert eine Übersicht über die erforderlichen Schritte für eine verteilte Installation.

Tabelle 1-28. Checkliste für die verteilte Bereitstellung

Aufgabe	Details
<input type="checkbox"/> Planen und Vorbereiten der Installationsumgebung und Überprüfen, ob alle Installationsvoraussetzungen erfüllt sind.	Vorbereitung für die Installation von vRealize Automation
<input type="checkbox"/> Planen und Beziehen Ihrer SSL-Zertifikate.	Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung
<input type="checkbox"/> Bereitstellen des Hauptservers der vRealize Automation-Appliance und zusätzlicher Appliances, die für die Redundanz und Hochverfügbarkeit erforderlich sind.	Bereitstellen der vRealize Automation-Appliance
<input type="checkbox"/> Konfigurieren Ihres Lastausgleichsdiensts für die Bewältigung des Datenverkehrs der vRealize Automation-Appliance.	Konfigurieren des Lastausgleichsdiensts
<input type="checkbox"/> Konfigurieren des Hauptservers der vRealize Automation-Appliance und zusätzlicher Appliances, die Sie für die Redundanz und Hochverfügbarkeit bereitgestellt haben.	Konfigurieren von Appliances für vRealize Automation
<input type="checkbox"/> Konfigurieren Ihres Lastausgleichsdiensts für die Bewältigung des Datenverkehrs der vRealize Automation-aaS-Komponente und Installieren der vRealize Automation-aaS-Komponenten.	Installieren deraaS-Komponenten in einer verteilten Konfiguration
<input type="checkbox"/> Bei Bedarf Installieren von Agents für die Integration in externe Systeme.	Installieren der vRealize Automation-Agents
<input type="checkbox"/> Konfigurieren des Standardmandanten und Bereitstellen deraaS-Lizenz.	Konfigurieren des Zugriffs auf den Standardmandanten

vRealize Orchestrator

Die vRealize Automation-Appliance enthält eine eingebettete Version von vRealize Orchestrator, die nun für Neuinstallationen empfohlen wird. Bei älteren Bereitstellungen oder für Spezialfälle können Benutzer jedoch vRealize Automation mit einer separaten, externen vRealize Orchestrator-Instanz verbinden. Weitere Informationen finden Sie unter <https://www.vmware.com/products/vrealize-orchestrator.html>.

Informationen zum Einrichten einer Verbindung zwischen vRealize Automation und vRealize Orchestrator finden Sie unter [VMware vRealize Orchestrator-Plug-In für vRealize Automation](#).

Verzeichnisverwaltung

Wenn Sie eine verteilte Installation mit Lastausgleichsdiensten für Hochverfügbarkeit und Failover installieren, benachrichtigen Sie das Team, das für die Konfiguration Ihrer vRealize Automation-Umgebung verantwortlich ist. Ihre Mandantenadministratoren müssen die Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren, wenn sie den Link zu Ihrem Active Directory konfigurieren.

Deaktivieren der Integritätsprüfungen des Lastausgleichsdiensts

Mithilfe von Integritätsprüfungen wird sichergestellt, dass ein Lastausgleichsdienst Datenverkehr nur an funktionierende Knoten sendet. Der Lastausgleichsdienst sendet Integritätsprüfungen entsprechend der festgelegten Häufigkeit an jeden Knoten. Knoten, die den Fehlerschwellenwert überschreiten, sind dann nicht mehr zum Empfang von neuen Datenverkehr berechtigt.

Zur Verteilung der Arbeitslast und für Failover können Sie mehrere vRealize Automation-Appliances hinter einem Lastausgleichsdienst platzieren. Außerdem können Sie mehrere IaaS-Webserver sowie mehrere IaaS-Manager-Dienst-Server hinter den entsprechenden Lastausgleichsdiensten platzieren.

Gestatten Sie den ggf. verwendeten Lastausgleichsdiensten nicht, Integritätsprüfungen jederzeit während des Installationsvorgangs zu senden. Integritätsprüfungen können die Installation stören oder zu einem unerwarteten Verhalten bei der Installation führen.

- Wenn Sie eine vRealize Automation-Appliance oder IaaS-Komponenten hinter vorhandenen Lastausgleichsdiensten bereitstellen, deaktivieren Sie die Integritätsprüfungen für alle Lastausgleichsdienste in der vorgeschlagenen Konfiguration, bevor Sie Komponenten installieren.
- Nach dem Installieren und Konfigurieren sämtlicher vRealize Automation-Komponenten, einschließlich aller vRealize Automation-Appliances und IaaS-Komponenten können Sie die Integritätsprüfungen wieder aktivieren.

Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung

vRealize Automation verwendet Zertifikate für die Pflege von Vertrauensbeziehungen und zum Bereitstellen von sicherer Kommunikation zwischen Komponenten in verteilten Bereitstellungen.

In einer verteilten oder Cluster-Bereitstellung entspricht die Zertifikatorganisation von vRealize Automation weitgehend der dreischichtigen Architektur von vRealize Automation. Die drei Schichten sind vRealize Automation-Appliance, IaaS-Website-Komponenten und Manager Service-Komponenten. In einem verteilten System teilen sich alle Hardwaremaschinen einer bestimmten Schicht ein Zertifikat. Das bedeutet, dass jede vRealize Automation-Appliance ein gemeinsames Zertifikat benutzt und jede Manager Service-Maschine das gemeinsame Zertifikat benutzt, das für die betreffende Schicht gilt.

Sie können vom System oder vom Benutzer generierte selbstsignierte Zertifikate oder von einer Zertifizierungsstelle bereitgestellte Zertifikate mit verteilten vRealize Automation-Bereitstellungen verwenden. Wenn der Benutzer keine Zertifikate bereitstellt, werden ab vRealize Automation 7.0 vom Installationsprogramm automatisch selbstsignierte Zertifikate für alle zutreffenden Knoten generiert und in den entsprechenden vertrauenswürdigen Speichern abgelegt.

Sie können Lastausgleichsdienste mit verteilten vRealize Automation-Komponenten verwenden, um Unterstützung für Hochverfügbarkeit und Failover zu bieten. VMware empfiehlt, für vRealize Automation-Bereitstellungen eine Pass-Through-Konfiguration für Bereitstellungen mit Lastausgleichsdiensten zu verwenden. In einer Pass-Through-Konfiguration reichen Lastausgleichsdienste Anforderungen an die entsprechenden Komponenten weiter, anstatt sie zu entschlüsseln. Die vRealize Automation-Appliance und die IaaS-Webserver müssen dann die notwendige Entschlüsselung durchführen.

Weitere Informationen zum Verwenden und Konfigurieren von Lastausgleichsdiensten finden Sie unter *vRealize Automation-Lastausgleich*.

Wenn Sie eigene Zertifikate bereitstellen oder mit Openssl oder einem anderen Tool generieren, können Sie entweder Platzhalter- oder SAN-Zertifikate (Subject Alternative Name) verwenden. Beachten Sie, dass es sich bei IaaS-Zertifikaten um mehrfach verwendbare Zertifikate handeln muss.

Falls Sie Zertifikate bereitstellen, müssen Sie ein mehrfach verwendbares Zertifikat anfordern, das die IaaS-Komponente im Cluster enthält, und dieses Zertifikat dann in den vertrauenswürdigen Speicher jeder Komponente kopieren. Wenn Sie Lastausgleichsdienste verwenden, müssen Sie den FQDN für den Lastausgleichsdienst in der vertrauenswürdigen Adresse des mehrfach verwendbaren Zertifikats des Clusters angeben.

Wenn Sie vom System generierte selbstsignierte Zertifikate mit vom Benutzer oder der Zertifizierungsstelle bereitgestellten Zertifikaten aktualisieren müssen, finden Sie weitere Informationen unter [Aktualisieren von vRealize Automation-Zertifikaten](#).

Die Tabelle „Anforderungen an vertrauenswürdige Zertifikate“ enthält eine Übersicht über die Registrierungsanforderungen der Vertrauensstellung für verschiedene importierte Zertifikate.

Tabelle 1-29. Anforderungen an vertrauenswürdige Zertifikate

Importieren	Registrieren
vRealize Automation-Appliance-Cluster	IaaS-Webkomponentencluster
IaaS-Webkomponentencluster	<ul style="list-style-type: none"> ■ vRealize Automation-Appliance-Cluster ■ Manager Service-Komponentencluster ■ DEM-Orchestrator- und DEM-Worker-Komponenten
Manager Service-Komponentencluster	<ul style="list-style-type: none"> ■ DEM-Orchestrator- und DEM-Worker-Komponenten ■ Agents und Proxy-Agents

Konfigurieren der Webkomponente, des Manager Service und des vertrauenswürdigen DEM-Hostzertifikats

Kunden, die einen Fingerabdruck mit vorinstallierten PFX-Dateien zur Unterstützung der Benutzerauthentifizierung verwenden, müssen einen vertrauenswürdigen Fingerabdruck auf dem Webhost und auf den Manager Service-, DEM Orchestrator- und DEM Worker-Hostmaschinen konfigurieren.

Kunden, die PEM-Dateien importieren oder selbstsignierte Zertifikate verwenden, können dieses Verfahren ignorieren.

Voraussetzungen

Für die Authentifizierung per Fingerabdruck verfügbare gültige Dateien `web.pfx` und `ms.pfx`.

Verfahren

- 1 Importieren Sie die Dateien `web.pfx` und `ms.pfx` in die folgenden Speicherorte auf den Webkomponenten- und Manager Service-Hostmaschinen:
 - `Host Computer/Certificates/Personal certificate store`
 - `Host Computer/Certificates/Trusted People certificate store`

- 2 Importieren Sie die Dateien `web.pfx` und `ms.pfx` in die folgenden Speicherorte auf den DEM Orchestrator- und DEM Worker-Hostmaschinen.

`Host Computer/Certificates/Trusted People certificate store`

- 3 Öffnen Sie ein Microsoft Management Console-Fenster auf jeder entsprechenden Hostmaschine.

Hinweis Die tatsächlichen Pfade und Optionen in der Management Console können je nach Windows-Version und Systemkonfiguration unterschiedlich sein.

- a Wählen Sie **Snap-In hinzufügen/entfernen** aus.
- b Wählen Sie **Zertifikate** aus.
- c Wählen Sie **Lokaler Computer** aus.
- d Öffnen Sie die Zertifikatdateien, die Sie zuvor importiert haben, und kopieren Sie die Fingerabdrücke.

Nächste Schritte

Fügen Sie den Fingerabdruck in die Seite „Zertifikat“ des vRealize Automation-Assistenten für den Manager Service, die Webkomponenten und die DEM-Komponenten ein.

Arbeitsblätter zur Installation

Arbeitsblätter dokumentieren wichtige Informationen, die während der Installation als Referenz erforderlich sind.

Für die Einstellungen ist die Groß-/Kleinschreibung zu beachten. Bitte beachten Sie dass es Platzhalter für weitere Komponenten gibt, wenn Sie eine verteilte Bereitstellung installieren. Sie brauchen möglicherweise nicht alle Platzhalter in den Arbeitsblättern. Darüber hinaus kann eine Maschine mehr als eine IaaS-Komponente hosten. So können der primäre Webserver und der DEM Orchestrator beispielsweise auf demselben FQDN sein.

Tabelle 1-30. vRealize Automation -Appliance

Variable	Mein Wert	Beispiel
FQDN der primären vRealize Automation-Appliance		automation.mycompany.com
IP-Adresse der primären vRealize Automation-Appliance		123.234.1.105
Nur als Referenz, geben Sie keine IP-Adressen ein.		
FQDN der zusätzlichen vRealize Automation-Appliance		automation2.mycompany.com
IP-Adresse der zusätzlichen vRealize Automation-Appliance		123.234.1.106
Nur als Referenz, geben Sie keine IP-Adressen ein.		

Tabelle 1-30. vRealize Automation -Appliance (Fortsetzung)

Variable	Mein Wert	Beispiel
FQDN des Lastausgleichsdiensts der vRealize Automation-Appliance		automation-balance.mycompany.com
IP-Adresse des Lastausgleichsdiensts der vRealize Automation-Appliance Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.201
Benutzername (https:// <i>appliance-FQDN</i> :5480) der Verwaltungsschnittstelle	Root (Standard)	root
Kennwort der Verwaltungsschnittstelle		admin123
Standardmandant	vsphere.local (Standard)	vsphere.local
Standardbenutzername des Mandanten	administrator@vsphere.local (Standard)	administrator@vsphere.local
Standardkennwort des Mandanten		login123

Tabelle 1-31. IaaS -Windows-Server

Variable	Mein Wert	Beispiel
Primärer IaaS-Webserver mit FQDN für Model Manager-Daten		web.mycompany.com
Primärer IaaS-Webserver mit IP-Adresse für Model Manager-Daten Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.107
Zusätzlicher FQDN für IaaS-Webserver		web2.mycompany.com
Zusätzliche IP-Adresse für IaaS-Webserver Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.108
FQDN des Lastausgleichsdiensts des IaaS-Webserver		web-balance.mycompany.com
IP-Adresse des Lastausgleichsdiensts des IaaS-Webserver Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.202
FQDN des aktiven IaaS-Manager Service-Hosts		mgr-svc.mycompany.com
IP-Adresse des aktiven IaaS-Manager Service-Hosts Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.109
FQDN des passiven IaaS-Manager Service-Hosts		mgr-svc2.mycompany.com

Tabelle 1-31. IaaS -Windows-Server (Fortsetzung)

Variable	Mein Wert	Beispiel
IP-Adresse des passiven IaaS-Manager Service-Hosts Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.110
FQDN des Lastausgleichsdiensts des IaaS-Manager Service-Hosts		mgr-svc-balance.mycompany.com
IP-Adresse des Lastausgleichsdiensts des IaaS-Manager Service-Hosts Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.203
Für IaaS-Dienste, Domänenkonto mit Administratorrechten auf Hosts		SUPPORT\provisioner
Kontokennwort		login123

Tabelle 1-32. IaaS -SQL Server-Datenbank

Variable	Mein Wert	Beispiel
Datenbankinstanz		IAASSQL
Datenbankname	vcac (Standard)	vcac
Passphrase (wird bei Installation, Upgrade und Migration verwendet)		login123

Tabelle 1-33. Distributed Execution Managers von IaaS

Variable	Mein Wert	Beispiel
FQDN des DEM-Hosts		dem.mycompany.com
IP-Adresse des DEM-Hosts Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.111
FQDN des DEM-Hosts		dem2.mycompany.com
IP-Adresse des DEM-Hosts Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.112
Eindeutiger Name des DEM Orchestrators		Orchestrator-1
Eindeutiger Name des DEM Orchestrators		Orchestrator-2
Eindeutiger Name des DEM Workers		Worker-1
Eindeutiger Name des DEM Workers		Worker-2
Eindeutiger Name des DEM Workers		Worker-3
Eindeutiger Name des DEM Workers		Worker-4

Konfigurieren des Lastausgleichsdiensts

Nachdem Sie die Appliances für vRealize Automation bereitgestellt haben, können Sie einen Lastausgleichsdienst einrichten, um den Datenverkehr auf mehrere Instanzen der vRealize Automation-Appliance zu verteilen.

Nachfolgend finden Sie eine Übersicht über die allgemeinen Schritte, die zum Konfigurieren eines Lastausgleichsdiensts für den vRealize Automation-Datenverkehr erforderlich sind:

- 1 Installieren Sie Ihren Lastausgleichsdienst.
- 2 Aktivieren Sie die Sitzungsaffinität (wird auch als „Sticky Sessions“ bezeichnet).
- 3 Stellen Sie sicher, dass die Zeitüberschreitung für den Lastausgleichsdienst mindestens 100 Sekunden beträgt.
- 4 Importieren Sie ein Zertifikat in Ihren Lastausgleichsdienst, falls Ihr Netzwerk oder Lastausgleichsdienst dies erfordert. Informationen zu Vertrauensstellungen und Zertifikaten finden Sie unter [Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung](#). Informationen zum Extrahieren von Zertifikaten finden Sie unter [Extrahieren von Zertifikaten und privaten Schlüsseln](#).
- 5 Konfigurieren Sie den Lastausgleichsdienst für den Datenverkehr der vRealize Automation-Appliance.
- 6 Konfigurieren Sie die Appliances für vRealize Automation. Siehe [Konfigurieren von Appliances für vRealize Automation](#).

Hinweis Wenn Sie virtuelle Appliances unter dem Lastausgleichsdienst einrichten, sollten Sie dies nur für virtuelle Appliances ausführen, die für die Verwendung mit vRealize Automation konfiguriert wurden. Wenn nicht konfigurierte Appliances eingerichtet werden, werden Fehlermeldungen angezeigt.

Weitere Informationen zu Lastausgleichsdiensten finden Sie unter [vRealize Automation-Lastausgleich](#).

Informationen zu Skalierbarkeit und Hochverfügbarkeit finden Sie im Handbuch *vRealize Automation-Referenzarchitektur*.

Konfigurieren von Appliances für vRealize Automation

Nach der Bereitstellung Ihrer Appliances und der Konfiguration des Lastausgleichsdiensts konfigurieren Sie die Appliances für vRealize Automation.

Konfigurieren der ersten vRealize Automation -Appliance in einem Cluster

Die vRealize Automation-Appliance ist eine teilweise konfigurierte virtuelle Maschine, die den Server und das Benutzer-Webportal von vRealize Automation hostet. Sie laden die Vorlage für das Open Virtualization Format (OVF) der Appliance auf vCenter Server oder die ESX/ESXi-Inventarliste herunter und stellen sie bereit.

Voraussetzungen

- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).

- Rufen Sie ein Authentifizierungszertifikat für die vRealize Automation-Appliance ab.

Wenn es für das Netzwerk oder den Lastausgleichsdienst erforderlich ist, wird das Zertifikat zu einem späteren Zeitpunkt in den Lastausgleichsdienst und weitere Appliances kopiert.

Verfahren

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

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

Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.

- 2 Wenn der Installationsassistent angezeigt wird, beenden Sie ihn, damit Sie anstelle des Assistenten zur Verwaltungsschnittstelle wechseln können.
- 3 Wählen Sie **Admin > Uhrzeiteinstellungen** aus und legen Sie die Quelle für die Uhrzeitsynchronisierung fest.

Option	Beschreibung
Hostuhrzeit	Mit ESXi-Host der vRealize Automation-Appliance synchronisieren.
Zeitserver	Mit externem Network Time Protocol (NTP)-Server synchronisieren. Geben Sie den FQDN oder die IP-Adresse des NTP-Servers ein.

Sie müssen alle vRealize Automation-Appliances und IaaS-Windows-Server mit derselben Zeitquelle synchronisieren. Verwenden Sie innerhalb einer vRealize Automation-Bereitstellung niemals verschiedene Zeitquellen.

- 4 Wählen Sie **vRA-Einstellungen > Hosteinstellungen** aus.

Option	Aktion
Automatisch lösen	Wählen Sie Automatisch lösen aus, um den Namen des aktuellen Hosts für die vRealize Automation-Appliance anzugeben.
Host aktualisieren	<p>Wählen Sie für neue Hosts die Option Host aktualisieren aus. Geben Sie den vollqualifizierten Domännennamen der vRealize Automation-Appliance, <code>vra-hostname.domain.name</code>, in das Textfeld Hostname ein.</p> <p>Wählen Sie für verteilte Bereitstellungen mit Lastausgleichsdiensten die Option Host aktualisieren aus. Geben Sie den vollqualifizierten Domännennamen für den Lastausgleichsserver, <code>vra-loadbalancername.domain.name</code>, in das Textfeld Hostname ein.</p>

Hinweis Konfigurieren Sie SSO-Einstellungen gemäß der Beschreibung weiter unten in diesem Verfahren immer dann, wenn Sie **Host aktualisieren** zum Festlegen des Hostnamens verwenden.

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.

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

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

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

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

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

- 6 Klicken Sie auf **Einstellungen speichern**, um Hostinformationen und SSL-Konfiguration zu speichern.
- 7 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**.
- 8 Konfigurieren Sie die SSO-Einstellungen.

9 Klicken Sie auf **Dienste**.

Alle Dienste müssen ausgeführt werden, bevor Sie eine Lizenz installieren oder sich bei der Konsole anmelden können. Die Dienste werden in der Regel nach etwa 10 Minuten gestartet.

Hinweis Sie können sich auch bei der Appliance anmelden und `tail -f /var/log/vcac/catalina.out` ausführen, um das Starten der Dienste zu überwachen.

10 Geben Sie Ihre Lizenzinformationen ein.

- a Klicken Sie auf **vRA-Einstellungen > Lizenzierung**.
- b Klicken Sie auf **Lizenzierung**.
- c Geben Sie einen gültigen vRealize Automation-Lizenzschlüssel ein, den Sie beim Herunterladen der Installationsdateien heruntergeladen haben, und klicken Sie auf **Schlüssel senden**.

Hinweis Wenn ein Verbindungsfehler auftritt, liegt möglicherweise ein Problem mit dem Lastausgleichsdienst vor. Überprüfen Sie die Netzwerkkonnektivität zum Lastausgleichsdienst.

11 Wählen Sie, ob vRealize Code Stream aktiviert werden soll, und geben Sie eine vRealize Code Stream-Lizenz ein.

vRealize Code Stream wird für Hochverfügbarkeits- oder Produktionsbereitstellungen von vRealize Automation nicht unterstützt.

12 Klicken Sie auf **Messaging**. Die Konfigurationseinstellungen und der Status des Messaging für Ihre Appliance werden angezeigt. Ändern Sie diese Einstellungen nicht.

13 Klicken Sie auf die Registerkarte **Telemetrie**, um auszuwählen, ob Sie am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program, CEIP) von VMware teilnehmen möchten.

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>.

- Aktivieren Sie **Join the VMware Customer Experience Improvement Program**, um an diesem Programm teilzunehmen.
- Deaktivieren Sie **Join the VMware Customer Experience Improvement Program**, um nicht an diesem Programm teilzunehmen.

14 Klicken Sie auf **Einstellungen speichern**.

15 Überprüfen Sie, ob Sie sich bei vRealize Automation anmelden können.

- a Öffnen Sie die URL für die vRealize Automation-Produktschnittstelle in einem Webbrowser.
`https://vrealize-automation-appliance-FQDN/vcac`
- b Ignorieren Sie ggf. etwaige Zertifikatswarnungen.
- c Melden Sie sich mit `administrator@vsphere.local` und dem Kennwort an, das Sie bei der Konfiguration von SSO angegeben haben.

Die Schnittstelle wird mit der Seite „Mandanten“ auf der Registerkarte **Administration** geöffnet. Ein einzelner Mandant mit dem Namen `vsphere.local` wird in der Liste angezeigt.

Konfigurieren zusätzlicher Instanzen der vRealize Automation -Appliance

Der Systemadministrator kann mehrere Instanzen der vRealize Automation-Appliance bereitstellen, um die Redundanz in einer Hochverfügbarkeitsumgebung sicherzustellen.

Für jede vRealize Automation-Appliance müssen Sie die Zeitsynchronisierung aktivieren und die Appliance zu einem Cluster hinzufügen. Konfigurationsinformationen basierend auf Einstellungen für die erste (primäre) vRealize Automation-Appliance werden automatisch hinzugefügt, wenn Sie die Appliance zum Cluster hinzufügen.

Wenn Sie eine verteilte Installation mit Lastausgleichsdiensten für Hochverfügbarkeit und Failover installieren, benachrichtigen Sie das Team, das für die Konfiguration Ihrer vRealize Automation-Umgebung verantwortlich ist. Ihre Mandantenadministratoren müssen die Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren, wenn sie den Link zu Ihrem Active Directory konfigurieren.

Hinzufügen einer weiteren vRealize Automation -Appliance zum Cluster

Zur Gewährleistung von Hochverfügbarkeit können verteilte Installationen einen Lastausgleichsdienst nutzen, der sich vor einem Cluster von vRealize Automation-Appliance-Knoten befindet.

Über die Verwaltungsschnittstelle der neuen vRealize Automation-Appliance fügen Sie den Knoten einem vorhandenen Cluster aus einer oder mehreren Appliances hinzu. Beim Beitrittsvorgang werden Konfigurationsinformationen auf die von Ihnen hinzugefügte neue Appliance kopiert. Hierzu zählen Zertifikat-, SSO-, Lizenzierungs-, Datenbank- und Messaging-Informationen.

Sie müssen die Appliances einem Cluster nacheinander und nicht parallel hinzufügen.

Voraussetzungen

- Der Cluster muss bereits einen oder mehrere vRealize Automation-Appliances enthalten, wobei eine der primäre Knoten ist. Siehe [Konfigurieren der ersten vRealize Automation-Appliance in einem Cluster](#).

Eine neue Appliance kann erst als primärer Knoten festgelegt werden, nachdem Sie sie dem Cluster hinzugefügt haben.
- Erstellen Sie den neuen Appliance-Knoten. Siehe [Bereitstellen der vRealize Automation-Appliance](#).
- Stellen Sie sicher, dass der Lastausgleichsdienst für die Verwendung mit der neuen Appliance konfiguriert ist.

- Überprüfen Sie, ob der Datenverkehr über den Lastausgleichsdienst geleitet werden kann, sodass er alle aktuellen Knoten und den neuen Knoten, den Sie hinzufügen möchten, erreicht.
- Stellen Sie sicher, dass alle vRealize Automation-Dienste auf den aktuellen Knoten gestartet wurden.

Verfahren

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

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

Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.

- 2 Wenn der Installationsassistent angezeigt wird, beenden Sie ihn, damit Sie anstelle des Assistenten zur Verwaltungsschnittstelle wechseln können.
- 3 Wählen Sie **Admin > Uhrzeiteinstellungen** aus und stellen Sie die Zeitquelle auf die gleiche ein, die auch in anderen Cluster-Appliances verwendet wird.
- 4 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 5 Geben Sie den FQDN einer zuvor konfigurierten vRealize Automation-Appliance in das Textfeld **Führender Clusterknoten** ein.

Sie können den FQDN der primären vRealize Automation-Appliance oder jeder anderen vRealize Automation-Appliance verwenden, die bereits zum Cluster hinzugefügt wurde.

- 6 Geben Sie das Root-Kennwort in das Textfeld **Kennwort** ein.
- 7 Klicken Sie auf **Cluster beitreten**.
- 8 Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.
Dienste für das Cluster werden neu gestartet.
- 9 Stellen Sie sicher, dass die Dienste ausgeführt werden.
 - a Klicken Sie auf die Registerkarte **Services**.
 - b Klicken Sie auf die Registerkarte **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Deaktivieren nicht verwendeter Dienste

Um interne Ressourcen in Fällen beizubehalten, in denen eine externe Instanz von vRealize Orchestrator verwendet wird, können Sie den eingebetteten vRealize Orchestrator-Dienst deaktivieren.

Voraussetzungen

[Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster](#)

Verfahren

- 1 Melden Sie sich bei der Konsole der vRealize Automation-Appliance an.

2 Beenden Sie den vRealize Orchestrator-Dienst.

```
service vco-server stop  
chkconfig vco-server off
```

Überprüfen der verteilten Bereitstellung

Nach dem Bereitstellen zusätzlicher Instanzen auf der vRealize Automation-Appliance überprüfen Sie, ob Sie auf die Appliances im Cluster zugreifen können.

Verfahren

- 1 Deaktivieren Sie vorübergehend alle Knoten in der Verwaltungsschnittstelle bzw. Konfigurationsdatei des Lastausgleichsdiensts mit Ausnahme des Knotens, den Sie überprüfen.
- 2 Bestätigen Sie, dass Sie sich über die Lastausgleichsdiensadresse bei vRealize Automation anmelden können:

`https://vrealize-automation-appliance-load-balancer-FQDN/vcac`
- 3 Nachdem Sie bestätigt haben, dass Sie die neue vRealize Automation-Appliance über den Lastausgleichsdienst aufrufen können, aktivieren Sie die anderen Knoten wieder.

Installieren der IaaS-Komponenten in einer verteilten Konfiguration

Der Systemadministrator installiert die IaaS-Komponenten, nachdem die Appliances bereitgestellt und vollständig konfiguriert wurden. Die IaaS-Komponenten ermöglichen den Zugriff auf Funktionen der vRealize Automation-Infrastruktur.

Alle Komponenten müssen unter demselben Dienstkonto ausgeführt werden, das ein Domänenkonto mit Rechten für jeden verteilten IaaS-Server sein muss. Verwenden Sie keine lokalen Systemkonten.

Voraussetzungen

- [Konfigurieren der ersten vRealize Automation-Appliance in einem Cluster](#).
- Wenn Ihre Site mehrere vRealize Automation-Appliances enthält, führen Sie die Schritte unter [Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster](#) aus.
- Stellen Sie sicher, dass der Server die unter [IaaS-Windows-Server](#) erläuterten Anforderungen erfüllt.
- Beziehen Sie ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle für den Import in den Zertifikatspeicher für vertrauenswürdige Stammzertifikate der Maschinen, auf denen Sie die Komponenten-Website- und Model Manager-Daten installieren möchten.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

Verfahren

1 [Installieren der IaaS-Zertifikate](#)

Rufen Sie für Produktionsumgebungen ein Domänenzertifikat von einer vertrauenswürdigen Zertifizierungsstelle ab. Importieren Sie das Zertifikat in den Zertifikatspeicher für vertrauenswürdige Stammzertifikate aller Maschinen, auf denen Sie die Website-Komponente und Manager Service (die IIS-Maschinen) bei der IaaS-Installation installieren möchten.

2 [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#)

Für die Installation von IaaS auf verteilten virtuellen oder physischen Windows-Servern laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

3 [Auswählen eines IaaS-Datenbankszenarios](#)

vRealize Automation IaaS verwendet eine Microsoft SQL Server-Datenbank, um Informationen zu den verwalteten Maschinen und zu den eigenen Elementen und Richtlinien zu warten.

4 [Installieren von IaaS-Website-Komponente und Model Manager-Daten](#)

Der Systemadministrator installiert die Website-Komponente, um Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole bereitzustellen. Sie können eine oder viele Instanzen der Website-Komponente installieren, aber Sie müssen Model Manager-Daten auf der Maschine konfigurieren, die die erste Website-Komponente hostet. Sie installieren Model Manager-Daten nur einmal.

5 [Installieren zusätzlicher IaaS-Webserver-Komponenten](#)

Der Webserver bietet Zugang zu Infrastrukturkapazitäten in vRealize Automation. Nach der Installation des ersten Webservers können Sie die Leistung erhöhen, indem Sie zusätzliche IaaS-Webserver installieren.

6 [Installieren der aktiven Manager Service-Komponente](#)

Der aktive Manager Service ist ein Windows-Dienst, der die Kommunikation zwischen Distributed Execution Manager-Instanzen, der Datenbank, den Agents, den Proxy-Agents und SMTP für IaaS koordiniert.

7 [Installieren einer Manager Service-Backup-Komponente](#)

Der Manager Service für Backups bietet Redundanz und Hochverfügbarkeit und kann manuell gestartet werden, wenn der aktive Dienst beendet wird.

8 [Installieren von Distributed Execution Managern](#)

Sie installieren den Distributed Execution Manager als eine von zwei Rollen: DEM-Orchestrator oder DEM-Worker. Sie müssen mindestens eine DEM-Instanz für jede Rolle installieren, und Sie können zusätzliche DEM-Instanzen für den Support von Failover und High Availability installieren.

9 [Konfigurieren des Windows-Diensts für den Zugriff auf die IaaS-Datenbank](#)

Ein Systemadministrator kann die Authentifizierungsmethode ändern, die für den Zugriff auf die SQL-Datenbank während der Laufzeit (nach Abschluss der Installation) verwendet wird. Standardmäßig wird die Windows-Identität des aktuell angemeldeten Kontos zur Verbindungsherstellung mit der Datenbank nach deren Installation verwendet.

10 Überprüfen der IaaS-Services

Nach der Installation stellt der Systemadministrator sicher, dass die IaaS-Dienste ausgeführt werden. Wenn die Dienste ausgeführt werden, war die Installation erfolgreich.

Nächste Schritte

Installieren Sie einen DEM-Orchestrator und mindestens eine DEM Worker-Instanz. Siehe [Installieren von Distributed Execution Managern](#).

Installieren der IaaS-Zertifikate

Rufen Sie für Produktionsumgebungen ein Domänenzertifikat von einer vertrauenswürdigen Zertifizierungsstelle ab. Importieren Sie das Zertifikat in den Zertifikatspeicher für vertrauenswürdige Stammzertifikate aller Maschinen, auf denen Sie die Website-Komponente und Manager Service (die IIS-Maschinen) bei der IaaS-Installation installieren möchten.

Voraussetzungen

Auf Windows 2012-Maschinen müssen Sie TLS1.2 für Zertifikate, die SHA512 verwenden, deaktivieren. Weitere Informationen zum Deaktivieren von TLS1.2 finden Sie im [Microsoft Knowledgebase-Artikel 245030](#).

Verfahren

- 1 Beziehen Sie ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle.
- 2 Öffnen Sie den Internetinformationsdienste-Manager.
- 3 Doppelklicken Sie in der Ansicht „Features“ auf **Serverzertifikate**.
- 4 Klicken Sie im Bereich „Aktionen“ auf **Importieren**.
 - a Geben Sie in das Textfeld **Zertifikatsdatei** einen Dateinamen ein oder klicken Sie auf die Schaltfläche zum Durchsuchen (...), um zu der Datei zu navigieren, in der das exportierte Zertifikat gespeichert ist.
 - b Geben Sie in das Textfeld **Kennwort** ein Kennwort ein, falls das Zertifikat mit einem Kennwort exportiert wurde.
 - c Wählen Sie **Schlüssel als exportierbar markieren** aus.
- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie auf das importierte Zertifikat und wählen Sie **Anzeigen** aus.
- 7 Stellen Sie sicher, dass das Zertifikat und die zugehörige Vertrauenskette vertrauenswürdig sind.

Wenn das Zertifikat nicht vertrauenswürdig ist, wird die Meldung **Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig** angezeigt.

Hinweis Sie müssen dieses Vertrauensstellungsproblem beheben, bevor Sie mit der Installation fortfahren können. Wenn Sie den Vorgang fortsetzen, schlägt Ihre Bereitstellung fehl.

- 8 Starten Sie IIS neu oder öffnen Sie ein Eingabeaufforderungsfenster mit erweiterten Berechtigungen und geben Sie `iisreset` ein.

Nächste Schritte

[Herunterladen des Installationsprogramms für vRealize Automation IaaS.](#)

Herunterladen des Installationsprogramms für vRealize Automation IaaS

Für die Installation von IaaS auf verteilten virtuellen oder physischen Windows-Servern laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

Voraussetzungen

- [Konfigurieren der ersten vRealize Automation-Appliance in einem Cluster](#) und optional [Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster](#).
- Stellen Sie sicher, dass der Server die unter [IaaS-Windows-Server](#) erläuterten Anforderungen erfüllt.
- Stellen Sie sicher, dass Sie ein Zertifikat zu IIS importiert haben und dass sich der Zertifikatsstamm oder die Zertifizierungsstelle im vertrauenswürdigen Stamm auf der Installationsmaschine befindet.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

Verfahren

- 1 (Optional) Aktivieren Sie HTTP, wenn Sie eine Installation auf eine Windows 2012-Maschine durchführen.
 - a Wählen Sie im Server-Manager **Features > Features hinzufügen** aus.
 - b Erweitern Sie in den .NET Framework-Funktionen die Option **WCF-Dienste**.
 - c Wählen Sie **HTTP-Aktivierung** aus.
- 2 Melden Sie sich auf dem IaaS-Windows-Server mit einem Konto mit Administratorrechten an.
- 3 Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance direkt in einem Webbrowser. Verwenden Sie keine Lastausgleichsdiensadresse.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 4 Klicken Sie auf **IaaS-Installationsprogramm**.
- 5 Speichern Sie `setup__vrealize-automation-appliance-FQDN@5480` auf dem Windows-Server. Ändern Sie den Dateinamen des Installationsprogramms nicht. Er wird verwendet, um die Installation mit der vRealize Automation-Appliance zu verbinden.
- 6 Laden Sie die Installationsdatei auf jeden IaaS-Windows-Server herunter, auf dem Sie Komponenten installieren.

Nächste Schritte

Informationen zum Installieren einer IaaS-Datenbank finden Sie unter [Auswählen eines IaaS-Datenbankszenarios](#).

Auswählen eines IaaS-Datenbankszenarios

vRealize Automation IaaS verwendet eine Microsoft SQL Server-Datenbank, um Informationen zu den verwalteten Maschinen und zu den eigenen Elementen und Richtlinien zu warten.

In Abhängigkeit von Ihren Einstellungen und Berechtigungen stehen mehrere Methoden zum Erstellen der IaaS-Datenbank zur Auswahl.

Hinweis Sie können sicheres SSL beim Erstellen oder beim Upgrade der SQL-Datenbank aktivieren. Beispielsweise können Sie beim Erstellen oder beim Upgrade der SQL-Datenbank mithilfe der Option für sicheres SSL festlegen, dass die bereits auf dem SQL Server angegebene SSL-Konfiguration beim Herstellen einer Verbindung mit der SQL-Datenbank verstärkt wird. SSL ermöglicht eine sicherere Verbindung zwischen dem IaaS-Server und der SQL-Datenbank. Für diese im benutzerdefinierten Installationsassistenten verfügbare Option muss SSL bereits auf dem SQL Server konfiguriert sein. Weitere Informationen zum Konfigurieren von SSL auf dem SQL-Server finden Sie im [Microsoft Technet-Artikel 189067](#).

Tabelle 1-34. Auswählen eines IaaS-Datenbankszenarios

Szenario	Prozedur
Manuelles Erstellen der IaaS-Datenbank mithilfe der bereitgestellten Datenbankskripts. Mithilfe dieser Option kann ein Datenbankadministrator die Änderungen vor dem Erstellen der Datenbank sorgfältig überprüfen.	Manuelles Erstellen der IaaS-Datenbank .
Vorbereiten einer leeren Datenbank und Auffüllen des Datenbankschemas mithilfe des Installationsprogramms. Diese Option ermöglicht es dem Installationsprogramm, einen Datenbankbenutzer mit dbo -Rechten zum Auffüllen der Datenbank zu verwenden.	Vorbereiten einer leeren Datenbank .
Erstellen der Datenbank mithilfe des Installationsprogramms. Dies ist die einfachste Option, erfordert jedoch die Verwendung von sysadmin -Rechten für das Installationsprogramm.	Erstellen der IaaS-Datenbank mithilfe des Installationsassistenten .

Manuelles Erstellen der IaaS-Datenbank

Der vRealize Automation-Systemadministrator kann die Datenbank mit von VMware bereitgestellten Skripts manuell erstellen.

Voraussetzungen

- Installieren Sie Microsoft .NET Framework 4.5.2 oder höher auf dem SQL Server-Host.
- Verwenden Sie die Windows-Authentifizierung anstelle der SQL-Authentifizierung, um eine Verbindung mit der Datenbank herzustellen.
- Überprüfen Sie die Installationsvoraussetzungen für die Datenbank. Siehe [IaaS SQL Server-Host](#).

- Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance in einem Webbrowser und laden Sie die IaaS-Datenbankinstallationskripte herunter.

<https://vrealize-automation-appliance-FQDN:5480/installer>

Verfahren

- 1 Navigieren Sie zum Database-Unterverzeichnis in dem Verzeichnis, in das Sie das ZIP-Archiv für die Installation extrahiert haben.
- 2 Extrahieren Sie das Archiv DBInstall.zip in ein lokales Verzeichnis.
- 3 Melden Sie sich am Windows-Datenbankhost mit entsprechenden Rechten an, um **sysadmin**-Rechte in der SQL Server-Instanz zu erstellen und zu löschen.
- 4 Überprüfen Sie ggf. die Skripts für die Datenbankbereitstellung. Überprüfen Sie insbesondere die Einstellungen im Abschnitt DBSettings von CreateDatabase.sql und bearbeiten Sie sie bei Bedarf.

Bei den Einstellungen im Skript handelt es sich um die empfohlenen Einstellungen. Nur `ALOW_SNAPSHOT_ISOLATION ON` und `READ_COMMITTED_SNAPSHOT ON` sind erforderlich.

- 5 Führen Sie den folgenden Befehl mit den in der Tabelle beschriebenen Argumenten aus.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Tabelle 1-35. Datenbankwerte

Variable	Wert
<i>db_server</i>	Gibt die SQL Server-Instanz im Format <code>dbhostname[,port number]\SQL instance</code> an. Geben Sie eine Portnummer nur an, wenn Sie einen nicht standardmäßigen Port verwenden. Die Microsoft SQL-Standardportnummer lautet 1433. Der Standardwert für <i>db_server</i> lautet <code>localhost</code> .
<i>db_name</i>	Der Name der Datenbank. Der Standardwert lautet <code>vra</code> . Datenbanknamen dürfen aus maximal 128 ASCII-Zeichen bestehen.
<i>db_dir</i>	Der Pfad zum Datenverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
<i>log_dir</i>	Der Pfad zum Protokollverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
<i>service_user</i>	Der Benutzername, unter dem der Manager Service ausgeführt wird.

Tabelle 1-35. Datenbankwerte (Fortsetzung)

Variable	Wert
<i>Web_user</i>	Der Benutzername, unter dem die Web Services ausgeführt werden.
<i>version_string</i>	Die vRealize Automation-Version. Sie wird angezeigt, wenn Sie sich bei der vRealize Automation-Appliance anmelden und auf die Registerkarte „Aktualisieren“ klicken. Beispiel für die Zeichenfolge der Version vRealize Automation 6.1: 6.1.0.1200.

Die Datenbank wird erstellt.

Nächste Schritte

[Installieren der IaaS-Komponenten in einer verteilten Konfiguration.](#)

Vorbereiten einer leeren Datenbank

Ein vRealize Automation-Systemadministrator kann das IaaS-Schema auf einer leeren Datenbank erstellen. Diese Installationsmethode bietet maximale Kontrolle über die Sicherheit der Datenbank.

Voraussetzungen

- Überprüfen Sie die Installationsvoraussetzungen für die Datenbank. Siehe [IaaS SQL Server-Host](#).
- Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance in einem Webbrowser und laden Sie die IaaS-Datenbankinstallationskripte herunter.

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

Verfahren

- 1 Navigieren Sie zum Verzeichnis Datenbank innerhalb des Verzeichnisses, in dem Sie das Installations-ZIP-Archiv extrahiert haben.
- 2 Extrahieren Sie das Archiv DBInstall.zip in ein lokales Verzeichnis.
- 3 Melden Sie sich beim Windows-Datenbankhost mit **sysadmin**-Berechtigungen innerhalb der SQL Server-Instanz an.
- 4 Bearbeiten Sie die folgenden Dateien und ersetzen Sie alle Instanzen der Variablen in der Tabelle durch die richtigen Werte für Ihre Umgebung.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

Tabelle 1-36. Datenbankwerte

Variable	Wert
<code>\$(DBName)</code>	Name der Datenbank, wie beispielsweise vra. Datenbanknamen dürfen aus maximal 128 ASCII-Zeichen bestehen.
<code>\$(DBDir)</code>	Der Pfad zum Datenverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
<code>\$(LogDir)</code>	Der Pfad zum Protokollverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.

- Prüfen Sie die Einstellungen im Abschnitt **Datenbankeinstellungen** von `SetDatabaseSettings.sql` und bearbeiten Sie diese bei Bedarf.

Die Einstellungen in dem Skript sind die empfohlenen Einstellungen für die IaaS-Datenbank. Es sind nur `ALLOW_SNAPSHOT_ISOLATION ON` und `READ_COMMITTED_SNAPSHOT ON` erforderlich.

- Öffnen Sie SQL Server Management Studio.
- Klicken Sie auf **Neue Abfrage**.
Es wird ein Fenster zur SQL-Abfrage geöffnet.
- Stellen Sie im Menü **Abfrage** sicher, dass **SQLCMD-Modus** ausgewählt ist.
- Fügen Sie den gesamten geänderten Inhalt von `CreateDatabase.sql` in das Abfragefenster ein.
- Fügen Sie unter dem Inhalt von `CreateDatabase.sql` den gesamten geänderten Inhalt von `SetDatabaseSettings.sql` hinzu.
- Klicken Sie auf **Ausführen**.

Das Skript wird ausgeführt und erstellt die Datenbank.

Nächste Schritte

[Installieren der IaaS-Komponenten in einer verteilten Konfiguration.](#)

Erstellen der IaaS-Datenbank mithilfe des Installationsassistenten

vRealize Automation verwendet eine Microsoft SQL Server-Datenbank, um Informationen zu den verwalteten Maschinen und zu den eigenen Elementen und Richtlinien zu warten.

Die folgenden Schritte beschreiben, wie Sie die IaaS-Datenbank mithilfe des Installationsprogramms erstellen oder wie Sie eine vorhandene leere Datenbank auffüllen. Die Datenbank kann auch manuell erstellt werden. Siehe [Manuelles Erstellen der IaaS-Datenbank](#).

Voraussetzungen

- Wenn Sie die Datenbank nicht mit der SQL-Authentifizierung, sondern mit der Windows-Authentifizierung erstellen, sollten Sie sicherstellen, dass der Benutzer, der das Installationsprogramm ausführt, über **sysadmin**-Rechte auf dem SQL Server verfügt.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS.](#)

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.
 - a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
 - b Wählen Sie **Zertifikat akzeptieren** aus.
 - c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.
- 7 Wählen Sie **laaS-Server** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.
- 8 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere laaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere laaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.
- 9 Klicken Sie auf **Weiter**.
- 10 Wählen Sie auf der Seite für die benutzerdefinierte Installation von laaS Server **Datenbank** aus.
- 11 Geben Sie im Textfeld **Datenbankinstanz** die Datenbankinstanz an oder klicken Sie auf **Durchsuchen** und wählen Sie eine Instanz aus der Liste aus. Wenn sich die Datenbankinstanz auf einem nicht standardmäßigen Port befindet, geben Sie in der Instanzspezifikation die Portnummer im Format `dbhost,SQL_port_number\SQLinstance` an. Die Microsoft SQL-Standardportnummer lautet 1443.
- 12 (Optional) Aktivieren Sie das Kontrollkästchen **SSL für Datenbankverbindung verwenden**.

Dieses Kontrollkästchen ist standardmäßig aktiviert. SSL ermöglicht eine sicherere Verbindung zwischen dem laaS-Server und der SQL-Datenbank. Sie müssen jedoch zunächst SSL auf dem SQL Server konfigurieren, damit diese Option unterstützt wird. Weitere Informationen zum Konfigurieren von SSL auf dem SQL-Server finden Sie im [Microsoft Technet-Artikel 189067](#).

13 Wählen Sie im Feld **Datenbankname** Ihren Datenbankinstallationstyp aus.

- Wählen Sie **Vorhandene leere Datenbank verwenden** aus, um das Schema in einer vorhandenen Datenbank zu erstellen.
- Geben Sie einen neuen Datenbanknamen ein oder verwenden Sie den Standardnamen **vra**, um eine neue Datenbank zu erstellen. Datenbanknamen dürfen aus maximal 128 ASCII-Zeichen bestehen.

14 Deaktivieren Sie **Standardmäßige Daten- und Protokollverzeichnisse verwenden**, um alternative Speicherorte anzugeben, oder lassen Sie diese Option aktiviert, um die Standardverzeichnisse zu verwenden (empfohlen).

15 Wählen Sie in der Liste **Authentifizierung** eine Authentifizierungsmethode für die Installation der Datenbank aus.

- Wählen Sie **Windows-Identität verwenden...** aus, um die Anmeldedaten, unter denen Sie das Installationsprogramm ausführen, zum Erstellen der Datenbank zu verwenden.
- Deaktivieren Sie **Windows-Identität verwenden...**, um die SQL-Authentifizierung zu verwenden. Geben Sie SQL-Anmeldedaten in die Textfelder für den Benutzernamen und das Kennwort ein.

Standardmäßig wird zur Laufzeit das Benutzerkonto des Windows-Diensts für den Zugriff auf die Datenbank verwendet. Dieses Benutzerkonto muss über sysadmin-Rechte für die SQL Server-Instanz verfügen. Für die Anmeldedaten, die zur Laufzeit für den Zugriff auf die Datenbank verwendet werden, kann die Verwendung von SQL-Anmeldedaten konfiguriert werden.

Die Windows-Authentifizierung wird empfohlen. Wenn Sie die SQL-Authentifizierung auswählen, wird das Kennwort für die unverschlüsselte Datenbank in bestimmten Konfigurationsdateien angezeigt.

16 Klicken Sie auf **Weiter**.

17 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
Keine Fehler	Klicken Sie auf Weiter .
Nicht kritische Fehler	Klicken Sie auf Umgehung .
Kritische Fehler	Durch Umgehen kritischer Fehler schlägt die Installation fehl. Wenn Warnungen angezeigt werden, wählen Sie die Warnung im linken Fensterbereich aus und folgen Sie den Anleitungen im rechten Bereich. Behandeln Sie alle kritischen Fehler und klicken Sie zum Überprüfen auf Erneut prüfen .

18 Klicken Sie auf **Installieren**.

19 Wenn die Erfolgsmeldung angezeigt wird, deaktivieren Sie **Anweisungen für Erstkonfiguration** und klicken Sie auf **Weiter**.

20 Klicken Sie auf **Beenden**.

Die Datenbank ist einsatzbereit.

Installieren von IaaS-Website-Komponente und Model Manager-Daten

Der Systemadministrator installiert die Website-Komponente, um Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole bereitzustellen. Sie können eine oder viele Instanzen der Website-Komponente installieren, aber Sie müssen Model Manager-Daten auf der Maschine konfigurieren, die die erste Website-Komponente hostet. Sie installieren Model Manager-Daten nur einmal.

Voraussetzungen

- Informationen zum Installieren der IaaS-Datenbank finden Sie unter [Auswählen eines IaaS-Datenbankszenarios](#).
- Wenn Sie bereits andere IaaS-Komponenten installiert haben, kennen Sie die Datenbank-Passphrase, die Sie erstellt haben.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

Verfahren

1 [Installieren der ersten IaaS-Webserver-Komponente](#)

Sie installieren die IaaS-Webserver-Komponente, um Zugang zu Infrastrukturkapazitäten in vRealize Automation zu bieten.

2 [Konfigurieren von Model Manager Data](#)

Sie installieren die Model Manager-Komponente auf derselben Maschine, auf der auch die erste Webserver-Komponente gehostet wird. Sie installieren die Model Manager-Daten nur einmal.

Sie können zusätzliche Website-Komponenten oder den Manager Service installieren. Siehe [Installieren zusätzlicher IaaS-Webserver-Komponenten](#) oder [Installieren der aktiven Manager Service-Komponente](#).

Installieren der ersten IaaS -Webserver-Komponente

Sie installieren die IaaS-Webserver-Komponente, um Zugang zu Infrastrukturkapazitäten in vRealize Automation zu bieten.

Sie können mehrere IaaS-Webserver installieren, allerdings enthält nur der erste Webserver Model Manager-Daten.

Voraussetzungen

- [Erstellen der IaaS-Datenbank mithilfe des Installationsassistenten](#).
- Stellen Sie sicher, dass der Server die unter [IaaS-Windows-Server](#) erläuterten Anforderungen erfüllt.
- Wenn Sie bereits andere IaaS-Komponenten installiert haben, kennen Sie die Datenbank-Passphrase, die Sie erstellt haben.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

Verfahren

- 1 Bei Verwendung eines Lastausgleichsdiensts deaktivieren Sie die anderen Knoten unter dem Lastausgleichsdienst und vergewissern sich, dass der Datenverkehr an den gewünschten Knoten weitergeleitet wird.

Deaktivieren Sie darüber hinaus Integritätsprüfungen des Lastausgleichsdiensts, bis alle vRealize Automation-Komponenten installiert und konfiguriert wurden.

- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.

- 3 Klicken Sie auf **Weiter**.

- 4 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

- 5 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

- a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

- b Wählen Sie **Zertifikat akzeptieren** aus.

- c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

- 6 Klicken Sie auf **Weiter**.

- 7 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

- 8 Wählen Sie **laaS-Server** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.

- 9 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere laaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere laaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

- 10 Klicken Sie auf **Weiter**.

- 11 Wählen Sie **Website** und **ModelManagerData** auf der Seite **Benutzerdefinierte Installation des laaS-Servers** aus.

- 12 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.

- 13 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.
- 14 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.
- 15 Wählen Sie das Zertifikat für diese Komponente aus.
 - a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
 - b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
 - c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen. Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom IaaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

- 16 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 17 (Optional) Wählen Sie **Zertifikatkonflikt unterdrücken** aus, um Zertifikatfehler zu unterdrücken. Die Installation ignoriert Fehler bei Zertifikatnamenskonflikten sowie Fehler bei Konflikten mit Remote-Zertifikatsperrlisten.

Diese Option ist weniger sicher.

Konfigurieren von Model Manager Data

Sie installieren die Model Manager-Komponente auf derselben Maschine, auf der auch die erste Webserver-Komponente gehostet wird. Sie installieren die Model Manager-Daten nur einmal.

Voraussetzungen

[Installieren der ersten IaaS-Webserver-Komponente.](#)

Verfahren

- 1 Klicken Sie auf die Registerkarte **Model Manager-Daten**.
- 2 Geben Sie im Textfeld **Server** den vollqualifizierten Domännennamen der vRealize Automation-Appliance ein.

vrealize-automation-appliance.mycompany.com

Geben Sie keine IP-Adresse ein.

- 3 Klicken Sie auf **Laden**, um den **Standardmandant für SSO** anzuzeigen.
Der Standardmandant `vsphere.local` wird beim Konfigurieren von Single Sign-On automatisch erstellt. Diesen Standardmandanten sollten Sie nicht ändern.
- 4 Klicken Sie auf **Herunterladen**, um das Zertifikat aus der virtuellen Appliance zu importieren.
Das Herunterladen des Zertifikats kann einige Minuten dauern.
- 5 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 6 Klicken Sie auf **Zertifikat akzeptieren**.
- 7 Geben Sie `administrator@vsphere.local` in das Textfeld **Benutzername** ein und geben Sie das Kennwort, das Sie bei der SSO-Konfiguration erstellt haben, in die Textfelder **Kennwort** und **Bestätigen** ein.
- 8 (Optional) Klicken Sie auf **Testen**, um die Anmeldedaten zu überprüfen.
- 9 Identifizieren Sie im Textfeld **laaS-Server** die laaS-Webserver-Komponente.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die laaS-Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die laaS Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 10 Klicken Sie auf **Testen**, um die Serververbindung zu überprüfen.
- 11 Klicken Sie auf **Weiter**.
- 12 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
Keine Fehler	Klicken Sie auf Weiter .
Nicht kritische Fehler	Klicken Sie auf Umgehung .
Kritische Fehler	Durch Umgehen kritischer Fehler schlägt die Installation fehl. Wenn Warnungen angezeigt werden, wählen Sie die Warnung im linken Fensterbereich aus und folgen Sie den Anleitungen im rechten Bereich. Behandeln Sie alle kritischen Fehler und klicken Sie zum Überprüfen auf Erneut prüfen .

- 13** Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

- 14** Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
Wenn Sie bereits Komponenten in dieser Umgebung installiert haben	Geben Sie die zuvor erstellte Passphrase in die Textfelder Passphrase und Bestätigen ein.
Wenn dies die erste Installation ist	Geben Sie eine Passphrase in die Textfelder Passphrase und Bestätigen ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

- 15** Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.

Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.

- 16** Klicken Sie auf **Weiter**.

- 17** Klicken Sie auf **Installieren**.

- 18** Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.

Nächste Schritte

Sie können zusätzliche Webserver-Komponenten oder den Manager Service installieren. Siehe [Installieren zusätzlicher IaaS-Webserver-Komponenten](#) oder [Installieren der aktiven Manager Service-Komponente](#).

Installieren zusätzlicher IaaS -Webserver-Komponenten

Der Webserver bietet Zugang zu Infrastrukturkapazitäten in vRealize Automation. Nach der Installation des ersten Webservers können Sie die Leistung erhöhen, indem Sie zusätzliche IaaS-Webserver installieren.

Installieren Sie keine Model Manager-Daten mit einer zusätzlichen Webserver-Komponente. Nur die erste Webserver-Komponente hostet Model Manager-Daten.

Voraussetzungen

- [Installieren von IaaS-Website-Komponente und Model Manager-Daten](#).
- Stellen Sie sicher, dass der neue Server die unter [IaaS-Windows-Server](#) erläuterten Anforderungen erfüllt.

- Ersetzen Sie das Zertifikat mithilfe der Verwaltungsschnittstelle der vRealize Automation-Appliance, um den FQDN des neuen Knotens aufzunehmen. Siehe [Ersetzen von Zertifikaten in der vRealize Automation-Appliance](#).
- Wenn Sie bereits andere IaaS-Komponenten installiert haben, kennen Sie die Datenbank-Passphrase, die Sie erstellt haben.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

Verfahren

- 1 Bei Verwendung eines Lastausgleichsdiensts deaktivieren Sie die anderen Knoten unter dem Lastausgleichsdienst und vergewissern sich, dass der Datenverkehr an den gewünschten Knoten weitergeleitet wird.

Deaktivieren Sie darüber hinaus Integritätsprüfungen des Lastausgleichsdiensts, bis alle vRealize Automation-Komponenten installiert und konfiguriert wurden.

- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.

- 3 Klicken Sie auf **Weiter**.

- 4 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

- 5 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

- a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

- b Wählen Sie **Zertifikat akzeptieren** aus.

- c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

- 6 Klicken Sie auf **Weiter**.

- 7 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

- 8 Wählen Sie **IaaS-Server** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.

- 9 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

- 10 Klicken Sie auf **Weiter**.
- 11 Wählen Sie **Website** auf der Seite **Benutzerdefinierte Installation des IaaS-Servers** aus.
- 12 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.
- 13 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.
- 14 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.
- 15 Wählen Sie das Zertifikat für diese Komponente aus.

- a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
- b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
- c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen.

Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom IaaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

- 16 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 17 (Optional) Wählen Sie **Zertifikatkonflikt unterdrücken** aus, um Zertifikatfehler zu unterdrücken. Die Installation ignoriert Fehler bei Zertifikatnamenskonflikten sowie Fehler bei Konflikten mit Remote-Zertifikatsperrlisten.

Diese Option ist weniger sicher.

- 18 Identifizieren Sie im Textfeld **IaaS-Server** die erste IaaS Webserver-Komponente.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die IaaS-Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die erste IaaS-Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 19 Klicken Sie auf **Testen**, um die Serververbindung zu überprüfen.
- 20 Klicken Sie auf **Weiter**.
- 21 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
Keine Fehler	Klicken Sie auf Weiter .
Nicht kritische Fehler	Klicken Sie auf Umgehung .
Kritische Fehler	Durch Umgehen kritischer Fehler schlägt die Installation fehl. Wenn Warnungen angezeigt werden, wählen Sie die Warnung im linken Fensterbereich aus und folgen Sie den Anleitungen im rechten Bereich. Behandeln Sie alle kritischen Fehler und klicken Sie zum Überprüfen auf Erneut prüfen .

- 22 Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

- 23 Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
Wenn Sie bereits Komponenten in dieser Umgebung installiert haben	Geben Sie die zuvor erstellte Passphrase in die Textfelder Passphrase und Bestätigen ein.
Wenn dies die erste Installation ist	Geben Sie eine Passphrase in die Textfelder Passphrase und Bestätigen ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

- 24 Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.

Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.

- 25 Klicken Sie auf **Weiter**.
- 26 Klicken Sie auf **Installieren**.
- 27 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.

Nächste Schritte

[Installieren der aktiven Manager Service-Komponente.](#)

Installieren der aktiven Manager Service-Komponente

Der aktive Manager Service ist ein Windows-Dienst, der die Kommunikation zwischen Distributed Execution Manager-Instanzen, der Datenbank, den Agents, den Proxy-Agents und SMTP für IaaS koordiniert.

Sofern Sie das automatische Manager Service-Failover nicht aktiviert haben, erfordert Ihre IaaS-Bereitstellung, dass der Manager Service jeweils auf nur einer Windows-Maschine aktiv ausgeführt wird. Auf Sicherungsmaschinen muss der Dienst beendet und für den manuellen Start konfiguriert werden.

Siehe [Informationen zum automatischen Manager Service-Failover](#).

Voraussetzungen

- Wenn Sie bereits andere IaaS-Komponenten installiert haben, kennen Sie die Datenbank-Passphrase, die Sie erstellt haben.
- (Optional) Wenn Sie den Manager Service in einer anderen Website als die Standardwebsite installieren möchten, erstellen Sie zuerst eine Website in den Internetinformationsdiensten.
- Stellen Sie sicher, dass Sie ein Zertifikat von einer Zertifizierungsstelle in IIS installiert haben, und dass das Stammzertifikat oder die Zertifizierungsstelle vertrauenswürdig sind. Alle Komponenten unter dem Lastausgleichsdienst müssen über dasselbe Zertifikat verfügen.
- Stellen Sie sicher, dass der Website-Lastausgleichsdienst konfiguriert ist und dass der Zeitüberschreitungswert für den Lastausgleichsdienst auf ein Minimum von 180 Sekunden festgelegt ist.
- [Installieren von IaaS-Website-Komponente und Model Manager-Daten](#).

Verfahren

- 1 Bei Verwendung eines Lastausgleichsdiensts deaktivieren Sie die anderen Knoten unter dem Lastausgleichsdienst und vergewissern sich, dass der Datenverkehr an den gewünschten Knoten weitergeleitet wird.

Deaktivieren Sie darüber hinaus Integritätsprüfungen des Lastausgleichsdiensts, bis alle vRealize Automation-Komponenten installiert und konfiguriert wurden.

- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

7 Wählen Sie **laaS-Server** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.

8 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere laaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere laaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

9 Klicken Sie auf **Weiter**.

10 Wählen Sie **Manager Service** auf der Seite **Benutzerdefinierte Installation des laaS-Servers** aus.

11 Identifizieren Sie im Textfeld **laaS-Server** die laaS-Webserver-Komponente.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die laaS-Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die laaS Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

12 Wählen Sie **Aktiver Knoten mit Starttyp Automatisch** aus.

13 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.

14 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.

15 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.

16 Wählen Sie das Zertifikat für diese Komponente aus.

- a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
- b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
- c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen. Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom IaaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

17 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.

18 Klicken Sie auf **Weiter**.

19 Überprüfen Sie die Voraussetzungen und klicken Sie auf **Weiter**.

20 Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

21 Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
Wenn Sie bereits Komponenten in dieser Umgebung installiert haben	Geben Sie die zuvor erstellte Passphrase in die Textfelder Passphrase und Bestätigen ein.
Wenn dies die erste Installation ist	Geben Sie eine Passphrase in die Textfelder Passphrase und Bestätigen ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

22 Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.

Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.

23 Klicken Sie auf **Weiter**.

24 Klicken Sie auf **Installieren**.

25 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.

26 Klicken Sie auf **Beenden**.

Nächste Schritte

- Um sicherzustellen, dass der installierte Manager Service die aktive Instanz ist, stellen Sie sicher, dass der vCloud Automation Center-Dienst ausgeführt wird und auf den Starttyp „Automatisch“ festgelegt ist.
- Sie können eine weitere Instanz der Manager Service-Komponente als eine passive Sicherung installieren, die Sie manuell starten können, wenn die aktive Instanz fehlschlägt. Siehe [Installieren einer Manager Service-Backup-Komponente](#).
- Ein Systemadministrator kann die Authentifizierungsmethode ändern, die für den Zugriff auf die SQL-Datenbank während der Laufzeit (nach Abschluss der Installation) verwendet wird. Siehe [Konfigurieren des Windows-Diensts für den Zugriff auf die IaaS-Datenbank](#).

Installieren einer Manager Service-Backup-Komponente

Der Manager Service für Backups bietet Redundanz und Hochverfügbarkeit und kann manuell gestartet werden, wenn der aktive Dienst beendet wird.

Sofern Sie das automatische Manager Service-Failover nicht aktiviert haben, erfordert Ihre IaaS-Bereitstellung, dass der Manager Service jeweils auf nur einer Windows-Maschine aktiv ausgeführt wird. Auf Sicherungsmaschinen muss der Dienst beendet und für den manuellen Start konfiguriert werden.

Siehe [Informationen zum automatischen Manager Service-Failover](#).

Voraussetzungen

- Wenn Sie bereits andere IaaS-Komponenten installiert haben, kennen Sie die Datenbank-Passphrase, die Sie erstellt haben.
- (Optional) Wenn Sie den Manager Service in einer anderen Website als die Standardwebsite installieren möchten, erstellen Sie zuerst eine Website in den Internetinformationsdiensten.
- Ersetzen Sie das Zertifikat mithilfe der Verwaltungsschnittstelle der vRealize Automation-Appliance, um den FQDN des neuen Knotens aufzunehmen. Siehe [Ersetzen von Zertifikaten in der vRealize Automation-Appliance](#).
- Stellen Sie sicher, dass Sie ein Zertifikat von einer Zertifizierungsstelle in IIS installiert haben, und dass das Stammzertifikat oder die Zertifizierungsstelle vertrauenswürdig sind. Alle Komponenten unter dem Lastausgleichsdienst müssen über dasselbe Zertifikat verfügen.
- Stellen Sie sicher, dass der Website-Lastausgleichsdienst konfiguriert ist.
- [Installieren von IaaS-Website-Komponente und Model Manager-Daten](#).

Verfahren

- 1 Bei Verwendung eines Lastausgleichsdiensts deaktivieren Sie die anderen Knoten unter dem Lastausgleichsdienst und vergewissern sich, dass der Datenverkehr an den gewünschten Knoten weitergeleitet wird.

Deaktivieren Sie darüber hinaus Integritätsprüfungen des Lastausgleichsdiensts, bis alle vRealize Automation-Komponenten installiert und konfiguriert wurden.

- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.

- 3 Klicken Sie auf **Weiter**.

- 4 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

- 5 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

- a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

- b Wählen Sie **Zertifikat akzeptieren** aus.

- c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

- 6 Klicken Sie auf **Weiter**.

- 7 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

- 8 Wählen Sie **IaaS-Server** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.

- 9 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

- 10 Klicken Sie auf **Weiter**.

- 11 Wählen Sie **Manager Service** auf der Seite **Benutzerdefinierte Installation des IaaS-Servers** aus.

12 Identifizieren Sie im Textfeld **laaS-Server** die laaS-Webserver-Komponente.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die laaS-Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die laaS Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 13 Wählen Sie **Verzögerter betriebsbereiter Knoten für Notfallwiederherstellung** aus.
- 14 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.
- 15 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.
- 16 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.
- 17 Wählen Sie das Zertifikat für diese Komponente aus.
 - a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
 - b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
 - c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen.

Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom laaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

- 18 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 19 Klicken Sie auf **Weiter**.
- 20 Überprüfen Sie die Voraussetzungen und klicken Sie auf **Weiter**.

- 21 Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

- 22 Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
Wenn Sie bereits Komponenten in dieser Umgebung installiert haben	Geben Sie die zuvor erstellte Passphrase in die Textfelder Passphrase und Bestätigen ein.
Wenn dies die erste Installation ist	Geben Sie eine Passphrase in die Textfelder Passphrase und Bestätigen ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

- 23 Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.

Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.

- 24 Klicken Sie auf **Weiter**.

- 25 Klicken Sie auf **Installieren**.

- 26 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.

- 27 Klicken Sie auf **Beenden**.

Nächste Schritte

- Um sicherzustellen, dass der installierte Manager Service eine passive Sicherungsinstanz ist, stellen Sie sicher, dass der vRealize Automation-Dienst nicht ausgeführt wird und auf den Starttyp „Manuell“ festgelegt ist.
- Ein Systemadministrator kann die Authentifizierungsmethode ändern, die für den Zugriff auf die SQL-Datenbank während der Laufzeit (nach Abschluss der Installation) verwendet wird. Siehe [Konfigurieren des Windows-Diensts für den Zugriff auf die IaaS-Datenbank](#).

Installieren von Distributed Execution Managern

Sie installieren den Distributed Execution Manager als eine von zwei Rollen: DEM-Orchestrator oder DEM-Worker. Sie müssen mindestens eine DEM-Instanz für jede Rolle installieren, und Sie können zusätzliche DEM-Instanzen für den Support von Failover und High Availability installieren.

Der Systemadministrator muss Installationsmaschinen auswählen, die vordefinierte Systemanforderungen erfüllen. Der DEM-Orchestrator und der -Worker können sich auf derselben Maschine befinden.

Wenn Sie die Installation von Distributed Execution Managern planen, beachten Sie die folgenden Überlegungen:

- DEM-Orchestratoren unterstützen Aktiv/Aktiv-High Availability. Normalerweise installieren Sie einen DEM-Orchestrator auf jeder Manager Service-Maschine.
- Installieren Sie den Orchestrator auf einer Maschine mit einer starken Netzwerkkonnektivität zum Model Manager-Host.
- Installieren Sie einen zweiten DEM-Orchestrator auf einer anderen Maschine für Failover.
- Normalerweise installieren Sie DEM-Worker auf dem IaaS Manager Service-Server oder auf einem separaten Server. Der Server muss über Netzwerkkonnektivität zum Model Manager-Host verfügen.
- Sie können zusätzliche DEM-Instanzen für Redundanz und Skalierbarkeit installieren, einschließlich mehrerer Instanzen auf derselben Maschine.

Es gibt bestimmte Anforderungen für die DEM-Installation, die von den verwendeten Endpoints abhängen. Siehe [IaaS Distributed Execution Manager-Host](#).

Installieren der Distributed Execution Manager

Sie müssen mindestens einen DEM-Worker und einen DEM-Orchestrator installieren. Der Installationsvorgang ist für beide Rollen identisch.

DEM-Orchestratoren unterstützen Aktiv/Aktiv-High Availability. Normalerweise installieren Sie einen einzelnen DEM-Orchestrator auf jeder Manager Service-Maschine. Sie können DEM-Orchestratoren und DEM-Worker auf derselben Maschine installieren.

Voraussetzungen

[Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

7 Wählen Sie **Distributed Execution Manager** unter „Komponentenauswahl“ auf der Seite für die Installationsarten aus.

8 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

9 Klicken Sie auf **Weiter**.

10 Überprüfen Sie die Voraussetzungen und klicken Sie auf **Weiter**.

11 Geben Sie die Anmeldedaten ein, unter denen der Dienst ausgeführt wird.

Das Dienstkonto erfordert lokale Administratorrechte und muss das Domänenkonto sein, das Sie während der IaaS-Installation verwendet haben. Das Dienstkonto verfügt über Rechte für jeden verteilten IaaS-Server und darf kein lokales Systemkonto sein.

12 Klicken Sie auf **Weiter**.

13 Wählen Sie aus dem Dropdown-Menü **DEM-Rolle** die Installationsart aus.

Option	Beschreibung
Worker	Der Worker führt Workflows aus.
Orchestrator	Der Orchestrator überwacht Aktivitäten des DEM-Workers, einschließlich der Planung und Vorverarbeitung von Workflows, sowie den Onlinestatus des DEM-Workers.

- 14 Geben Sie einen eindeutigen Namen in das Textfeld **DEM-Name** ein, der diesen DEM identifiziert.

Der Name darf keine Leerzeichen enthalten und nicht länger als 128 Zeichen sein. Wenn Sie einen zuvor verwendeten Namen eingeben, wird die folgende Meldung angezeigt: „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.“

- 15 (Optional) Geben Sie eine Beschreibung dieser Instanz in **DEM-Beschreibung** ein.
- 16 Geben Sie die Hostnamen und Ports in die Textfelder **Manager Service-Hostname** und **Hostname des Model Manager-Webdiensts** ein.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente und den Webserver ein, der den Model Manager hostet, <i>mgr-svc-load-balancer.mycompany.com:443</i> und <i>web-load-balancer.mycompany.com:443</i> . Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der die Manager Service-Komponente und der Webserver installiert wurden, der den Model Manager hostet, <i>mgr-svc.mycompany.com:443</i> und <i>web.mycompany.com:443</i> . Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 17 (Optional) Klicken Sie auf **Testen** zum Testen der Verbindungen zu Manager Service und dem Model Manager-Webdienst.
- 18 Klicken Sie auf **Hinzufügen**.
- 19 Klicken Sie auf **Weiter**.
- 20 Klicken Sie auf **Installieren**.
- 21 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.
- 22 Klicken Sie auf **Beenden**.

Nächste Schritte

- Stellen Sie sicher, dass der Dienst ausgeführt wird und dass das Protokoll keine Fehler anzeigt. Der Dienstname ist VMware DEM *Rolle – Name*. Rolle ist Orchestrator oder Worker. Der Protokollspeicherort ist *Installationspfad*\Distributed Execution Manager\Name\Protokolle.
- Wiederholen Sie diesen Vorgang zum Installieren zusätzlicher DEM-Instanzen.

Konfigurieren des DEM zur Herstellung der Verbindung zu SCVMM auf einem anderen Installationspfad

Standardmäßig verwendet die DEM Worker-Konfigurationsdatei den Standardinstallationspfad der Konsole von Microsoft System Center Virtual Machine Manager (SCVMM). Wenn Sie die SCVMM-Konsole an einem nicht standardmäßigen Speicherort installieren, müssen Sie die Datei aktualisieren.

Dieses Verfahren muss nur durchgeführt werden, wenn Sie über SCVMM-Endpoints und -Agents verfügen.

Voraussetzungen

- Behalten Sie den nicht standardmäßigen Pfad in Erinnerung, in dem Sie die SCVMM-Konsole installiert haben.

Folgender Pfad ist der Standardpfad, der in der Konfigurationsdatei ersetzt werden muss.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

Verfahren

1 Beenden des DEM Worker-Dienstprogramms.

2 Öffnen Sie die folgende Datei in einem Texteditor.

Programmdateien (x86)\VMware\vCAC\Distributed Execution Manager*Instanzname*\DynamicOps.DEM.exe.config

3 Suchen Sie den Abschnitt <assemblyLoadConfiguration>.

4 Aktualisieren Sie jeden Pfad gemäß dem folgenden Beispiel.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

5 Speichern und schließen Sie DynamicOps.DEM.exe.config.

6 Starten Sie den DEM Worker-Dienst erneut.

Weitere Informationen finden Sie unter [DEM-Worker mit SCVMM](#).

Weitere Informationen zur Vorbereitung der SCVMM-Umgebung und Erstellung eines SCVMM-Endpoints finden Sie in [Vorbereiten Ihrer SCVMM-Umgebung](#) und [Erstellen eines Hyper-V \(SCVMM\)-Endpoints](#).

Konfigurieren des Windows-Diensts für den Zugriff auf die IaaS-Datenbank

Ein Systemadministrator kann die Authentifizierungsmethode ändern, die für den Zugriff auf die SQL-Datenbank während der Laufzeit (nach Abschluss der Installation) verwendet wird. Standardmäßig wird die Windows-Identität des aktuell angemeldeten Kontos zur Verbindungsherstellung mit der Datenbank nach deren Installation verwendet.

Aktivieren des Zugriffs auf die IaaS-Datenbank über den Dienstbenutzer

Wenn die SQL-Datenbank vom Manager Service auf einem separaten Host installiert wird, muss der Zugriff auf die Datenbank über den Manager Service aktiviert werden. Wenn der Benutzername, unter dem der Manager Service ausgeführt wird, der Besitzer der Datenbank ist, so ist keine Aktion erforderlich. Wenn der Benutzer nicht der Besitzer der Datenbank ist, muss der Systemadministrator den Zugriff gewähren.

Voraussetzungen

- [Auswählen eines IaaS-Datenbankszenarios](#).
- Stellen Sie sicher, dass der Benutzername, unter dem der Manager Service ausgeführt werden soll, nicht der Besitzer der Datenbank ist.

Verfahren

- 1 Navigieren Sie innerhalb des Verzeichnisses, in das Sie das ZIP-Archiv für die Installation extrahiert haben, zum Database-Unterverzeichnis.
- 2 Extrahieren Sie das Archiv DBInstall.zip in ein lokales Verzeichnis.
- 3 Melden Sie sich beim Datenbankhost als ein Benutzer mit der **sysadmin**-Rolle in der SQL Server-Instanz an.
- 4 Bearbeiten Sie VMPS0psUser.sql und ersetzen Sie alle Instanzen von \$(Service User) mit dem Benutzer (aus Schritt 3), unter dem der Manager Service ausgeführt werden soll.
Ersetzen Sie ServiceUser am Zeilenende nicht durch WHERE name = N'ServiceUser').
- 5 Öffnen Sie SQL Server Management Studio.
- 6 Wählen Sie im linken Bereich unter **Datenbanken** die Datenbank aus (standardmäßig vCAC).
- 7 Klicken Sie auf **Neue Abfrage**.
Im rechten Bereich wird ein Fenster zur SQL-Abfrage geöffnet.
- 8 Fügen Sie den geänderten Inhalt von VMPS0psUser.sql in das Abfragefenster ein.
- 9 Klicken Sie auf **Ausführen**.

Der Zugriff auf die Datenbank über den Manager Service ist aktiviert.

Konfigurieren des Kontos der Windows-Dienste zur Verwendung von SQL-Authentifizierung

Standardmäßig greift das Konto der Windows-Dienste während der Laufzeit auf die Datenbank zu, selbst wenn Sie die Datenbank mit SQL-Authentifizierung konfiguriert haben. Sie können die Laufzeit-Authentifizierung von Windows zu SQL ändern.

Ein Grund zur Änderung der Laufzeit-Authentifizierung könnte beispielsweise sein, dass sich die Datenbank in einer nicht vertrauenswürdigen Domäne befindet.

Voraussetzungen

Vergewissern Sie sich, ob die vRealize Automation SQL Server-Datenbank vorhanden ist. Beginnen Sie mit [Auswählen eines IaaS-Datenbankszenarios](#).

Verfahren

- 1 Melden Sie sich mit einem Konto mit Administratorrechten bei dem IaaS-Windows-Server an, der den Manager Service hostet.
- 2 Beenden Sie in **Verwaltung > Dienste** den **VMware vCloud Automation Center**-Dienst.
- 3 Öffnen Sie folgende Dateien in einem Texteditor.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config  
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 Suchen Sie in jeder Datei den Abschnitt <connectionStrings>.
- 5 Ersetzen Sie
`Integrated Security=True;`
mit
`User Id=Datenbank-Benutzername;Password=Datenbank-Kennwort;`
- 6 Speichern und schließen Sie die Dateien.

```
ManagerService.exe.config  
Web.config
```

- 7 Starten Sie den **VMware vCloud Automation Center**-Dienst.
- 8 Starten Sie IIS mit dem Befehl `iisreset neu`.

Überprüfen der IaaS-Services

Nach der Installation stellt der Systemadministrator sicher, dass die IaaS-Dienste ausgeführt werden. Wenn die Dienste ausgeführt werden, war die Installation erfolgreich.

Verfahren

- 1 Wählen Sie aus dem Windows Desktop der IaaS-Maschine die Option **Verwaltung > Dienste** aus.
- 2 Suchen Sie die folgenden Dienste und stellen Sie sicher, dass der Status jeweils „Gestartet“ lautet und der Starttyp auf „Automatisch“ festgelegt ist.
 - VMware DEM – Orchestrator – *Name*, wo *Name* die Zeichenfolge darstellt, die im Feld **DEM-Name** während der Installation zur Verfügung gestellt wurde.
 - VMware DEM – Worker – *Name*, wo *Name* die Zeichenfolge darstellt, die im Feld **DEM-Name** während der Installation zur Verfügung gestellt wurde.

- *Agent name* des Agents von VMware vCloud Automation Center
- VMware vCloud Automation Center-Dienst

3 Schließen Sie das Fenster **Dienste**.

Installieren der vRealize Automation -Agents

vRealize Automation verwendet Agents für die Integration in externe Systeme. Ein Systemadministrator kann zu installierende Agents zum Kommunizieren mit anderen Virtualisierungsplattformen auswählen.

vRealize Automation verwendet die folgenden Agenttypen zum Verwalten von externen Systemen:

- Hypervisor-Proxy-Agents (vSphere, Citrix Xen-Server und Microsoft Hyper-V-Server)
- EPI-Integrations-Agents (External Provisioning Infrastructure)
- VDI-Agents (Virtual Desktop Infrastructure)
- WMI-Agents (Windows Management Instrumentation)

Sie können für High Availability mehrere Agents für einen einzelnen Endpoint installieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie sie gleich. Redundante Agents bieten etwas Fehlertoleranz, aber kein Failover. Wenn Sie beispielsweise zwei vSphere-Agents installieren, einen auf Server A und einen auf Server B, und Server A nicht mehr zur Verfügung steht, verarbeitet der auf Server B installierte Agent die Arbeitselemente weiterhin. Allerdings kann der Agent auf Server B die Verarbeitung eines Arbeitselements nicht beenden, die der Agent auf Server A bereits gestartet hat.

Sie können einen vSphere-Agent als Teil der Minimalinstallation installieren, aber nach der Installation können Sie auch andere Agents hinzufügen, einschließlich eines zusätzlichen vSphere-Agents. In einer verteilten Bereitstellung können Sie alle Agents nach der Fertigstellung der verteilten Basisinstallation installieren. Die zu installierenden Agents sind von den Ressourcen in der Infrastruktur abhängig.

Weitere Informationen zur Verwendung von vSphere-Agents finden Sie unter [vSphere Agent-Anforderungen](#).

Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned

Sie müssen die PowerShell-Ausführungsrichtlinie von „Eingeschränkt“ auf „RemoteSigned“ oder „Nicht eingeschränkt“ festlegen, damit lokale PowerShell-Skripts ausgeführt werden können.

Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie im [Microsoft PowerShell-Artikel über Ausführungsrichtlinien](#). Wenn Ihre PowerShell-Ausführungsrichtlinie auf der Ebene der Gruppenrichtlinien verwaltet wird, wenden Sie sich an den IT-Support, um Informationen zu den geltenden Einschränkungen bei Richtlinienänderungen zu erhalten, und lesen Sie den [Microsoft PowerShell-Artikel über Gruppenrichtlinieneinstellungen](#).

Voraussetzungen

- Stellen Sie vor der Agent-Installation sicher, dass Microsoft PowerShell auf dem Installationshost installiert ist. Die erforderliche Version hängt vom Betriebssystem des Installationshosts ab. Informieren Sie sich unter „Hilfe und Support“ von Microsoft.

- Um weitere Informationen zur PowerShell-Ausführungsrichtlinie zu erhalten, führen Sie `help about_signing` oder `help Set-ExecutionPolicy` bei der PowerShell-Eingabeaufforderung aus.

Verfahren

- 1 Melden Sie sich mit einem Administratorkonto bei der IaaS-Hostmaschine an, auf der der Agent installiert ist.
- 2 Wählen Sie **Start > Alle Programme > Windows PowerShell-Version > Windows PowerShell**.
- 3 Führen Sie für „Remote signiert“ `Set-ExecutionPolicy RemoteSigned` aus.
- 4 Führen Sie für „Nicht eingeschränkt“ `Set-ExecutionPolicy Unrestricted` aus.
- 5 Prüfen Sie, ob der Befehl zu keinerlei Fehlern geführt hat.
- 6 Geben Sie bei der PowerShell-Eingabeaufforderung **Exit** ein.

Auswählen des Agent-Installationsszenarios

Die Agents, die Sie installieren müssen, hängen von den externen Systemen ab, für die Sie eine Integration planen.

Tabelle 1-37. Auswählen eines Agent-Szenarios

Integrationszenario	Agent-Anforderungen und Vorgehensweisen
Bereitstellung von Cloud-Maschinen durch die Integration in eine Cloud-Umgebung wie beispielsweise Amazon Web Services oder Red Hat Enterprise Linux OpenStack Platform.	Es muss kein Agent installiert werden.
Bereitstellung virtueller Maschinen durch die Integration in eine vSphere-Umgebung.	Installieren und Konfigurieren des Proxy-Agents für vSphere
Bereitstellung virtueller Maschinen durch die Integration in eine Microsoft Hyper-V Server-Umgebung.	Installieren des Proxy-Agents für Hyper-V oder XenServer
Bereitstellung virtueller Maschinen durch die Integration in eine XenServer-Umgebung.	<ul style="list-style-type: none"> ■ Installieren des Proxy-Agents für Hyper-V oder XenServer ■ Installieren des EPI-Agents für Citrix
Bereitstellung virtueller Maschinen durch die Integration in eine XenDesktop-Umgebung.	<ul style="list-style-type: none"> ■ Installieren des VDI-Agents für XenDesktop ■ Installieren des EPI-Agents für Citrix
Ausführung von Visual Basic-Skripts als zusätzliche Schritte im Bereitstellungsprozess vor oder nach der Bereitstellung einer Maschine oder während der Aufhebung der Bereitstellung.	Installieren des EPI-Agents für Visual Basic-Skripterstellung
Erfassen von Daten von den bereitgestellten Windows-Maschinen, beispielsweise der Active Directory-Status des Besitzers einer Maschine.	Installieren des WMI-Agents für WMI-Remoteanforderungen
Bereitstellung virtueller Maschinen durch die Integration in jede andere unterstützte virtuelle Plattform.	Es muss kein Agent installiert werden.

Installationsspeicherort und Anforderungen für Agents

Der Systemadministrator installiert die Agents in der Regel auf dem vRealize Automation-Server, der die aktive Manager Service-Komponente hostet.

Wenn ein Agent auf einem anderen Host installiert wird, muss die Netzwerkkonfiguration die Kommunikation zwischen dem Agent und der Manager Services-Installationsmaschine erlauben.

Jeder Agent wird unter einem eindeutigen Namen in einem eigenen Verzeichnis, `Agents\Agent_Name`, des Installationsverzeichnisses von vRealize Automation (in der Regel `Programme (x86)\VMware\re\VCAC`) installiert, wobei die Konfiguration in der `VRMAgent.exe.config` in diesem Verzeichnis gespeichert wird.

Installieren und Konfigurieren des Proxy-Agents für vSphere

Ein Systemadministrator installiert Proxy-Agents zum Kommunizieren mit vSphere-Server-Instanzen. Die Agents ermitteln vorhandene Arbeit, rufen Hostinformationen ab und melden abgeschlossene Arbeitselemente und andere Hoststatusänderungen.

vSphere Agent-Anforderungen

vSphere Endpoint-Anmeldedaten oder die Anmeldedaten, unter denen der Agent-Dienst ausgeführt wird, müssen über Administratorzugriff auf den Installationshost verfügen. Mehrere vSphere-Agents müssen die Konfigurationsanforderungen für vRealize Automation erfüllen.

Anmeldedaten

Beim Erstellen eines Endpoints, der die vom vSphere-Agent zu verwaltende vCenter Server-Instanz darstellt, kann der Agent die Anmeldedaten verwenden, mit denen der Dienst ausgeführt wird, um mit dem vCenter Server zu interagieren bzw. separate Endpoint-Anmeldedaten anzugeben.

In der folgenden Tabelle sind die erforderlichen Berechtigungen für die Anmeldedaten des vSphere-Endpoints zur Verwaltung einer vCenter Server-Instanz aufgeführt. Die Berechtigungen müssen für alle Cluster in vCenter Server und nicht nur für Cluster, von denen Endpoints gehostet werden, aktiviert sein.

Tabelle 1-38. Erforderliche Berechtigungen an vSphere -Agents für die Verwaltung von vCenter Server -Instanzen

Attributwert	Berechtigung
Datenspeicher	Speicher zuteilen
	Datenspeicher durchsuchen
Datenspeicher-Cluster	Konfigurieren eines Datenspeicher-Clusters
Ordner	Ordner erstellen
	Ordner löschen
Global	Benutzerdefinierte Attribute verwalten
	Benutzerdefiniertes Attribut festlegen
Netzwerk	Netzwerk zuweisen
Berechtigungen	Berechtigung ändern
Ressourcen	Ressourcenpool VMs zuweisen
	Ausgeschaltete virtuelle Maschine migrieren
	Eingeschaltete virtuelle Maschine migrieren

Tabelle 1-38. Erforderliche Berechtigungen an vSphere -Agents für die Verwaltung von vCenter Server -Instanzen (Fortsetzung)

Attributwert		Berechtigung
Virtuelle Maschine	Bestandsliste	Aus vorhandener erstellen
		Neue erstellen
		Verschieben
		Entfernen
	Interaktion	CD-Medien konfigurieren
		Konsoleninteraktion
		Geräteverbindung
		Ausschalten
		Einschalten
		Zurücksetzen
		Anhalten
		Tools installieren
	Konfiguration	Vorhandene Festplatte hinzufügen
		Neue Festplatte hinzufügen
		Gerät hinzufügen oder entfernen
		Festplatte entfernen
		Erweitert
		CPU-Anzahl ändern
		Ressourcen ändern
		Virtuelle Festplatte erweitern
		Festplattenänderungsverfolgung
		Arbeitsspeicher
		Geräteeinstellungen ändern
		Umbenennen
		Anmerkung festlegen (Version 5.0 und höher)
		Einstellungen
	Platzierung der Auslagerungsdatei	
	Bereitstellung	Anpassen
		Vorlage klonen
		Virtuelle Maschine klonen
		Vorlage bereitstellen
		Anpassungsspezifikationen lesen
	Zustand	Snapshot erstellen

Tabelle 1-38. Erforderliche Berechtigungen an vSphere -Agents für die Verwaltung von vCenter Server -Instanzen (Fortsetzung)

Attributwert	Berechtigung
	Snapshot entfernen
	Snapshot wiederherstellen

Führen Sie die Deaktivierung oder Neukonfiguration von jeder Drittanbietersoftware durch, die den Betriebszustand von virtuellen Maschinen außerhalb von vRealize Automation ändern kann. Solche Änderungen können die Verwaltung des Lebenszyklus der Maschine durch vRealize Automation beeinträchtigen.

Installieren des vSphere -Agents

Installieren Sie einen vSphere-Agent zum Verwalten von vCenter Server-Instanzen. Für High Availability können Sie einen zweiten, redundanten vSphere-Agent für dieselbe vCenter Server-Instanz installieren. Sie müssen beide vSphere-Agents gleich benennen und konfigurieren und sie auf verschiedenen Maschinen installieren.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- Stellen Sie sicher, dass sich die Maschine, auf der der Agent installiert ist, auf einer Domäne befindet, der die Domäne, auf der die IaaS-Komponenten installiert sind, vertraut.
- Überprüfen Sie, ob die Anforderungen in [vSphere Agent-Anforderungen](#) erfüllt werden.
- Wenn Sie bereits einen vSphere-Endpoint für die Verwendung mit diesem Agent erstellt haben, notieren Sie sich den Namen des Endpoints.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS.](#)

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

6 Wählen Sie im Bereich „Komponentenauswahl“ **Proxy-Agents**.

7 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

8 Klicken Sie auf **Weiter**.

9 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie vSphere aus der Liste **Agenttyp** aus.

12 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

13 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

14 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

15 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

16 Geben Sie den Namen des Endpoints ein.

Der Endpoint-Name, den Sie in vRealize Automation konfigurieren, muss mit dem Endpoint-Namen übereinstimmen, der bei der Installation für den vSphere-Proxy-Agent angegeben wurde. Andernfalls ist der Endpoint nicht funktionsfähig.

17 Klicken Sie auf **Hinzufügen**.

18 Klicken Sie auf **Weiter**.

19 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

20 Klicken Sie auf **Weiter**.

21 Klicken Sie auf **Beenden**.

22 Überprüfen Sie, ob die Installation erfolgreich war.

23 (Optional) Fügen Sie mehrere Agents mit unterschiedlichen Konfigurationen und einen Endpoint auf dasselbe System hinzu.

Nächste Schritte

[Konfigurieren des vSphere-Agents.](#)

Konfigurieren des vSphere -Agents

Konfigurieren Sie den vSphere-Agent als Vorbereitung für das Erstellen und Verwenden von vSphere-Endpoints in vRealize Automation-Blueprints.

Ändern Sie mithilfe des Proxy-Agent-Dienstprogramms verschlüsselte Teile der Agent-Konfigurationsdatei oder die Löschroutine der Maschine für Virtualisierungsplattformen. Nur ein Teil der Agent-Konfiguration `VRMAgent.exe.config` ist verschlüsselt. So ist beispielsweise der Abschnitt `serviceConfiguration` nicht verschlüsselt.

Voraussetzungen

Melden Sie sich mit einem Konto mit Administratorrechten bei dem IaaS-Windows-Server an, auf dem Sie den vSphere-Agent installiert haben.

Verfahren

- 1 Öffnen Sie als Administrator eine Windows-Eingabeaufforderung.
- 2 Wechseln Sie zum Agent-Installationsordner, wobei *agent-name* der Ordner mit dem vSphere-Agent ist.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\agent-name
```

- 3 (Optional) Um die aktuellen Konfigurationseinstellungen anzuzeigen, geben Sie folgenden Befehl ein.
`DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get`

Im Folgenden finden Sie ein Beispiel für diesen Befehl.

```
managementEndpointName: VCendpoint  
doDeletes: True
```

- 4 (Optional) Um den Namen des Endpoints zu ändern, den Sie bei der Installation konfiguriert haben, geben Sie folgenden Befehl ein.

```
set managementEndpointName
```

Zum Beispiel: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

Benennen Sie mit diesem Verfahren den Endpoint innerhalb von vRealize Automation um, anstatt Endpoints zu ändern.

- 5 (Optional) Um die Löschroutine der virtuellen Maschine zu konfigurieren, geben Sie folgenden Befehl ein.

```
set doDeletes
```

Beispiel: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

Option	Beschreibung
Wahr	(Standard) Löschen Sie die von vCenter Server in vRealize Automation gelöschten virtuellen Maschinen.
Falsch	Verschieben Sie virtuelle Maschinen, die in vRealize Automation gelöscht wurden, ins Verzeichnis VRMDeleted in vCenter Server.

- 6 Öffnen Sie **Verwaltung > Dienste** und starten Sie den vRealize Automation Agent-Dienst – *agent-name* neu.

Nächste Schritte

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

Installieren des Proxy-Agents für Hyper-V oder XenServer

Ein Systemadministrator installiert Proxy-Agents zum Kommunizieren mit Hyper-V- und XenServer-Server-Instanzen. Die Agents ermitteln vorhandene Arbeit, rufen Hostinformationen ab und melden abgeschlossene Arbeitselemente und andere Hoststatusänderungen.

Hyper-V - und XenServer -Anforderungen

Hyper-V-Hypervisor-Proxy-Agents erfordern Systemadministrator-Anmeldedaten für die Installation.

Die Anmeldedaten, unter denen der Agent-Dienst ausgeführt wird, benötigen Administratorzugriff auf den Installationshost.

Administratoranmeldedaten sind für alle XenServer- oder Hyper-V-Instanzen auf den Hosts erforderlich, die vom Agent verwaltet werden sollen.

Wenn Sie Xen-Pools verwenden, müssen alle Knoten im Xen-Pool durch ihre vollqualifizierten Domänennamen identifiziert werden.

Hinweis Standardmäßig ist Hyper-V nicht für die Remoteverwaltung konfiguriert. Ein vRealize Automation Hyper-V-Proxy-Agent kann nur mit einem Hyper-V-Server kommunizieren, wenn die Remoteverwaltung aktiviert wurde.

Informationen zum Konfigurieren von Hyper-V für die Remoteverwaltung finden Sie in der Dokumentation zu Microsoft Windows Server.

Installieren des Hyper-V- oder XenServer-Agents

Der Hyper-V-Agent verwaltet Hyper-V-Server-Instanzen. Der XenServer-Agent verwaltet XenServer-Server-Instanzen.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).
- Stellen Sie sicher, dass Hyper-V-Hypervisor-Proxy-Agents über Anmeldedaten für den Systemadministrator verfügen.
- Stellen Sie sicher, dass die Anmeldedaten, unter denen der Agent-Dienst ausgeführt wird, über Administratorzugriff auf den Installationshost verfügen.
- Stellen Sie sicher, dass alle XenServer- oder Hyper-V-Instanzen auf den Hosts durch den Agent mit Anmeldedaten auf Administratorebene verwaltet werden.

- Beachten Sie bei der Verwendung von Xen-Pools, dass alle Knoten innerhalb des Xen-Pools durch ihren vollqualifizierten Domännennamen identifiziert werden müssen.

vRealize Automation kann nicht mit einem Knoten kommunizieren bzw. keinen Knoten verwalten, der nicht durch seinen vollqualifizierten Domännennamen innerhalb des Xen-Pools identifiziert wird.

- Konfigurieren Sie Hyper-V für Remoteverwaltung, um die Hyper-V-Serverkommunikation mit vRealize Automation Hyper-V-Proxy-Agents zu aktivieren.

Informationen zum Konfigurieren von Hyper-V für die Remoteverwaltung finden Sie in der Dokumentation zu Microsoft Windows Server.

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.
 - a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.
Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
 - b Wählen Sie **Zertifikat akzeptieren** aus.
 - c Klicken Sie auf **Zertifikat anzeigen**.
Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.
- 5 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.
- 6 Wählen Sie **Komponentenauswahl** auf der Seite für die Installationsarten aus.

- 7 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

- 8 Klicken Sie auf **Weiter**.

- 9 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.

- 10 Klicken Sie auf **Weiter**.

- 11 Wählen Sie den Agent aus der Liste **Agenttyp** aus.

- Xen
- Hyper-V

- 12 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

- 13 Übermitteln Sie den **Agent-Namen** an den IaaS-Administrator, der Endpoints konfiguriert.

Der Endpoint muss für die Aktivierung des Zugriffs und der Datenerfassung mit dem Agent verknüpft werden, der für ihn konfiguriert wurde.

14 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

15 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

16 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

17 Geben Sie die Anmeldedaten eines Benutzers mit Berechtigungen auf Administratorebene auf der verwalteten Server-Instanz ein.

18 Klicken Sie auf **Hinzufügen**.

19 Klicken Sie auf **Weiter**.

20 (Optional) Fügen Sie einen weiteren Agent hinzu.

Sie können beispielsweise einen Xen-Agent hinzufügen, wenn Sie zuvor den Hyper-V-Agent hinzugefügt haben.

21 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

22 Klicken Sie auf **Weiter**.

23 Klicken Sie auf **Beenden**.

24 Überprüfen Sie, ob die Installation erfolgreich war.

Nächste Schritte

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

[Konfigurieren des Hyper-V- oder XenServer-Agents.](#)

Konfigurieren des Hyper-V - oder XenServer -Agents

Der Systemadministrator kann die Konfigurationseinstellungen für den Proxy-Agent ändern, wie beispielsweise die Löschroutine für Virtualisierungsplattformen. Mit dem Proxy-Agent-Dienstprogramm können Sie die Erstkonfigurationen ändern, die in der Agent-Konfigurationsdatei verschlüsselt sind.

Voraussetzungen

Melden Sie sich als **Systemadministrator** an der Maschine an, auf der Sie den Agent installiert haben.

Verfahren

- 1 Wechseln Sie zum Installationsverzeichnis des Agents, wobei *Agent_Name* das Verzeichnis mit dem Proxy-Agent ist. Dies ist auch der Name, unter dem der Agent installiert wird.

```
cd Programme (x86)\VMware\vCAC Agents\Agent_Name
```

- 2 Zeigen Sie die aktuellen Konfigurationseinstellungen an.

Geben Sie Folgendes ein: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get`

Nachfolgend finden Sie ein Beispiel für die Befehlsausgabe:

```
Benutzername: XAdmin
```

- 3 Geben Sie den Befehl `set` ein, um eine Eigenschaft zu ändern, wobei *Eigenschaft* für eine der in der Tabelle aufgeführten Optionen steht.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set Eigenschaft Wert
```

Wenn Sie keine Angabe für *Wert* machen, werden Sie zur Eingabe eines neuen Werts aufgefordert.

Eigenschaft	Beschreibung
username	Der Benutzername bezeichnet Administratoranmeldedaten für den XenServer oder Hyper-V Server, mit dem der Agent kommuniziert.
password	Das Kennwort für den Administratorbenutzernamen.

- 4 Klicken Sie auf **Start > Verwaltung > Dienste** und starten Sie den Dienst vRealize Automation-Agent – *Agent_Name* neu.

Beispiel: Ändern der Administratoranmeldedaten

Geben Sie den folgenden Befehl ein, um die bei der Agent-Installation angegebenen Administratoranmeldedaten für die Virtualisierungsplattform zu ändern.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Nächste Schritte

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

Installieren des VDI-Agents für XenDesktop

vRealize Automation verwendet VDI-PowerShell-Agents (Virtual Desktop Integration) zum Registrieren der XenDesktop-Maschinen, die es mit externen Desktopverwaltungssystemen bereitstellt.

Der VDI-Integrations-Agent stellt für die Besitzer von registrierten Maschinen eine direkte Verbindung zur XenDesktop-Web-Schnittstelle bereit. Sie können einen VDI-Agent als einen festgelegten Agent zum Interagieren mit einem einzelnen Desktop Delivery Controller (DDC) oder als einen allgemeinen Agent installieren, der mit mehreren DDCs interagieren kann.

XenDesktop-Anforderungen

Ein Systemadministrator installiert einen virtuellen Desktopinfrastruktur-Agent (VDI-Agent), um XenDesktop-Server in vRealize Automation zu integrieren.

Sie können einen allgemeinen VDI-Agent zur Interaktion mit mehreren Servern installieren. Wenn Sie pro Server einen individuellen Agent für den Lastausgleich oder die Autorisierung installieren, müssen Sie bei der Installation des Agents den Namen des XenDesktop DDC-Servers angeben. Ein individueller Agent kann nur Registrierungsanforderungen verarbeiten, die an den in seiner Konfiguration angegebenen Server übermittelt werden.

Auf der VMware-Website unter *Übersicht über die Unterstützung von vRealize Automation* finden Sie weitere Informationen zu unterstützten Versionen von XenDesktop für XenDesktop DDC-Server.

Installationshost und Anmeldedaten

Die Anmeldedaten, mit denen der Agent ausgeführt wird, müssen über Administratorzugriff auf alle XenDesktop DDC-Server verfügen, mit denen er interagiert.

XenDesktop-Anforderungen

Der Name, der dem XenServer-Host auf Ihrem XenDesktop-Server gegeben wurde, muss mit der UUID des Xen-Pools in XenCenter übereinstimmen. Weitere Informationen hierzu finden Sie unter [Festlegen des XenServer-Hostnamens](#).

Jeder XenDesktop DDC-Server, mit dem Sie Maschinen registrieren möchten, muss folgendermaßen konfiguriert werden:

- Der Gruppen- bzw. Katalogtyp muss zur Verwendung mit vRealize Automation auf **Vorhanden** festgelegt sein.
- Der Name eines vCenter Server-Hosts auf einem DDC-Server muss mit dem Namen auf der vCenter Server-Instanz übereinstimmen, wie er auf dem vRealize Automation vSphere-Endpoint eingegeben wurde (ohne Domäne). Der Endpoint muss mit einem vollqualifizierten Domännennamen (FQDN), nicht jedoch mit einer IP-Adresse, konfiguriert werden. Wenn die Adresse auf dem Endpoint z. B. „https://virtual-center27.domain/sdk“ lautet, muss der Name des Hosts auf dem DDC-Server auf „virtual-center27“ festgelegt werden.

Wenn Ihr vRealize Automation vSphere-Endpoint mit einer IP-Adresse konfiguriert wurde, müssen Sie dies ändern und einen FQDN verwenden. Weitere Informationen zum Einrichten von Endpoints finden Sie unter *IaaS-Konfiguration*.

Anforderungen an XenDesktop-Agent-Host

Citrix XenDesktop SDK muss installiert sein. Das SDK für XenDesktop ist auf XenDesktop-Installationsmedium enthalten.

Stellen Sie vor der Agent-Installation sicher, dass Microsoft PowerShell auf dem Installationshost installiert ist. Die erforderliche Version hängt vom Betriebssystem des Installationshosts ab. Informieren Sie sich unter „Hilfe und Support“ von Microsoft.

Die MS PowerShell-Ausführungsrichtlinie ist auf RemoteSigned oder Unrestricted festgelegt. Siehe [Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned](#).

Um weitere Informationen zur PowerShell-Ausführungsrichtlinie zu erhalten, führen Sie `help about_signing` oder `help Set-ExecutionPolicy` bei der PowerShell-Eingabeaufforderung aus.

Festlegen des XenServer-Hostnamens

In XenDesktop muss der Name, der dem XenServer-Host auf Ihrem XenDesktop-Server gegeben wurde, mit der UUID des Xen-Pool in XenCenter übereinstimmen. Wenn kein Xen-Pool konfiguriert wurde, muss der Name mit der UUID des XenServer selbst übereinstimmen.

Verfahren

- 1 Wählen Sie in Citrix XenCenter Ihren Xen-Pool oder eigenständigen XenServer aus und klicken Sie auf die Registerkarte **Allgemein**. Notieren Sie sich die UUID.
- 2 Wenn Sie Ihren XenServer-Pool oder eigenständigen Host zu XenDesktop hinzufügen, geben Sie die im vorherigen Schritt notierte UUID als Name für **Verbindung** ein.

Installieren des XenDesktop-Agents

VDI-PowerShell-Agents (Virtual Desktop Integration) lässt sich in externe virtuelle Desktopsysteme, wie beispielsweise XenDesktop und Citrix, einbinden. Verwenden Sie einen VDI-PowerShell-Agent zum Verwalten der XenDesktop-Maschine.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- Überprüfen Sie, ob die Anforderungen in [XenDesktop-Anforderungen](#) erfüllt werden.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.
 - a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
 - b Wählen Sie **Zertifikat akzeptieren** aus.
 - c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.
- 7 Wählen Sie **Proxy-Agents** im Fensterbereich für die Komponentenauswahl aus.
- 8 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.
- 9 Klicken Sie auf **Weiter**.
- 10 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.
- 11 Klicken Sie auf **Weiter**.
- 12 Wählen Sie **VdiPowerShell** aus der Liste **Agenttyp** aus.

- 13 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

- 14 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 15 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

- 16 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

- 17 Wählen Sie die **VDI-Version** aus.

- 18 Geben Sie den vollqualifizierten Domännennamen des verwalteten Servers in das Textfeld **VDI-Server** ein.

- 19 Klicken Sie auf **Hinzufügen**.

20 Klicken Sie auf **Weiter**.

21 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

22 Klicken Sie auf **Weiter**.

23 Klicken Sie auf **Beenden**.

24 Überprüfen Sie, ob die Installation erfolgreich war.

25 (Optional) Fügen Sie mehrere Agents mit unterschiedlichen Konfigurationen und einen Endpoint auf dasselbe System hinzu.

Nächste Schritte

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

Installieren des EPI-Agents für Citrix

EPI-PowerShell-Agents (External Provisioning Integration) integrieren externe Citrix-Maschinen in den Bereitstellungsvorgang. Der EPI-Agent bietet On-Demand-Streaming der Citrix-Datenträger-Images, von denen aus die Maschinen starten und ausgeführt werden.

Der festgelegte EPI-Agent interagiert mit einem einzelnen externen Bereitstellungsserver. Sie müssen einen EPI-Agent für jede Serverinstanz der Citrix-Bereitstellung installieren.

Anforderungen an Citrix Provisioning Server

Der Systemadministrator verwendet EPI-Agents (External Provisioning Infrastructure), um Citrix Provisioning Server zu integrieren und die Verwendung von Visual Basic-Skripts beim Bereitstellungsprozess zu ermöglichen.

Installationsspeicherort und Anmeldedaten

Installieren Sie den Agent auf dem PVS-Host für Citrix Provisioning Services-Instanzen. Stellen Sie sicher, dass der Installationshost die [Anforderungen an den Citrix-Agent-Host](#) erfüllt, bevor Sie den Agent installieren.

Ein EPI-Agent kann zwar im Allgemeinen mit mehreren Servern interagieren, aber für Citrix Provisioning Server ist ein dedizierter EPI-Agent erforderlich. Sie müssen für jede Citrix Provisioning Server-Instanz einen EPI-Agent installieren und den Namen des Hostservers angeben. Die Anmeldedaten, mit denen der Agent ausgeführt wird, benötigen Administratorzugriff auf die Citrix Provisioning Server-Instanz.

In der *Übersicht über die Unterstützung von vRealize Automation* finden Sie weitere Informationen zu den unterstützten Versionen von Citrix PVS.

Anforderungen an den Citrix-Agent-Host

PowerShell und Citrix Provisioning Services SDK müssen auf dem Installationshost installiert werden, bevor Sie den Agent installieren. Ausführliche Informationen hierzu finden Sie in der *Übersicht über die Unterstützung von vRealize Automation* auf der VMware-Website.

Stellen Sie vor der Agent-Installation sicher, dass Microsoft PowerShell auf dem Installationshost installiert ist. Die erforderliche Version hängt vom Betriebssystem des Installationshosts ab. Informieren Sie sich unter „Hilfe und Support“ von Microsoft.

Darüber hinaus müssen Sie sicherstellen, dass das PowerShell-Snap-In installiert ist. Weitere Informationen hierzu finden Sie im *Programmiererhandbuch für Citrix Provisioning Services und PowerShell* auf der Citrix-Website.

Die MS PowerShell-Ausführungsrichtlinie ist auf RemoteSigned oder Unrestricted festgelegt. Siehe [Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned](#).

Um weitere Informationen zur PowerShell-Ausführungsrichtlinie zu erhalten, führen Sie `help about_signing` oder `help Set-ExecutionPolicy` bei der PowerShell-Eingabeaufforderung aus.

Installieren des Citrix-Agents

Mit EPI-PowerShell-Agents (External Provisioning Integration) können Sie externe Systeme in den Maschinenbereitstellungsvorgang integrieren. Verwenden Sie den EPI-PowerShell-Agent zum Integrieren in den Citrix-Bereitstellungsserver, um die Bereitstellung von Maschinen durch On-Demand-Disk-Streaming zu aktivieren.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- Überprüfen Sie, ob die Anforderungen in [Anforderungen an Citrix Provisioning Server](#) erfüllt werden.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

6 Wählen Sie **Komponentenauswahl** auf der Seite für die Installationsarten aus.

7 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

8 Klicken Sie auf **Weiter**.

9 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie **EPIPowerShell** aus der Liste für den Agenttyp aus.

12 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

13 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

14 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

15 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

16 Wählen Sie den EPI-Typ aus.

17 Geben Sie den vollqualifizierten Domännennamen des verwalteten Servers in das Textfeld **EPI-Server** ein.

18 Klicken Sie auf **Hinzufügen**.

19 Klicken Sie auf **Weiter**.

20 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

21 Klicken Sie auf **Weiter**.

22 Klicken Sie auf **Beenden**.

23 Überprüfen Sie, ob die Installation erfolgreich war.

24 (Optional) Fügen Sie mehrere Agents mit unterschiedlichen Konfigurationen und einen Endpoint auf dasselbe System hinzu.

Nächste Schritte

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

Installieren des EPI-Agents für Visual Basic-Skripterstellung

Ein Systemadministrator kann Visual Basic-Skripts als zusätzliche Schritte im Bereitstellungsvorgang angeben. Dies kann vor, während oder nach der Bereitstellung einer Maschine erfolgen. Sie müssen vor dem Ausführen von Visual Basic-Skripts einen EPI-PowerShell-Agent (External Provisioning Integration) installieren.

Visual Basic-Skripts werden in dem Blueprint angegeben, von dem aus Maschinen bereitgestellt werden. Diese Skripts haben Zugriff auf alle benutzerdefinierten Eigenschaften, die mit den Maschinen verknüpft sind, und können deren Werte aktualisieren. Der nächste Schritt in dem Workflow hat Zugriff auf diese neuen Werte.

Sie können beispielsweise mit einem Skript Zertifikate oder Sicherheitstoken vor der Bereitstellung erstellen und diese bei der Maschinenbereitstellung verwenden.

Um Skripts in der Bereitstellung zu aktivieren, müssen Sie einen bestimmten Typ eines EPI-Agents installieren und die zu verwendenden Skripts auf dem System positionieren, auf dem der Agent installiert ist.

Bei der Ausführung eines Skripts leitet der EPI-Agent alle benutzerdefinierten Eigenschaften der Maschine als Argumente an das Skript weiter. Um aktualisierte Eigenschaftswerte zurückzugeben, müssen Sie diese Eigenschaften in einem Wörterbuch positionieren und eine vRealize Automation-Funktion aufrufen. Ein Beispielskript ist im Unterverzeichnis des Installationsverzeichnisses des EPI-Agents des Skripts enthalten. Dieses Skript enthält eine Überschrift zum Laden aller Argumente in ein Wörterbuch, einen Text, in den Sie die Funktion(en) hinzufügen können, und eine Fußzeile zum Zurückgeben der benutzerdefinierten Eigenschaftswerte.

Hinweis Sie können mehrere EPI/VBSkripts-Agents auf mehreren Servern installieren und mit einem bestimmten Agent und den Visual Basic-Skripts auf dem Host dieses Agents bereitstellen. Wenden Sie sich in diesem Fall an den VMware-Kundensupport.

Anforderungen für Visual Basic-Skripterstellung

Ein Systemadministrator installiert externe Bereitstellungsinfrastruktur-Agents (EPI-Agents), um die Verwendung von Visual Basic-Skripts beim Bereitstellungsprozess zu aktivieren.

In der folgenden Tabelle werden die Anforderungen beschrieben, die für die Installation eines EPI-Agent zur Aktivierung der Verwendung von Visual Basic-Skripts beim Bereitstellungsprozess gelten.

Tabelle 1-39. EPI-Agents für Visual Scripting

Anforderung	Beschreibung
Anmeldedaten	Die Anmeldedaten, mit denen der Agent ausgeführt wird, müssen über Administratorzugriff auf den Installationshost verfügen.
Microsoft PowerShell	Die Installation von Microsoft PowerShell auf dem Installationshost muss vor der Installation auf dem Agent erfolgen. Die erforderliche Version hängt vom Betriebssystem des Installationshosts ab und wurde möglicherweise mit diesem Betriebssystem installiert. Weitere Informationen finden Sie unter http://support.microsoft.com .
MS PowerShell-Ausführungsrichtlinie	Die MS-PowerShell-Ausführungsrichtlinie muss auf RemoteSigned oder Nicht eingeschränkt festgelegt sein. Geben Sie für Informationen zur PowerShell-Ausführungsrichtlinie einen der folgenden Befehle an der PowerShell-Eingabeaufforderung aus:
	<pre>help about_signing help Set-ExecutionPolicy</pre>

Installieren des Agents für Visual Basic-Skripterstellung

Mit EPI-PowerShell-Agents (External Provisioning Integration) können Sie externe Systeme in den Maschinenbereitstellungsvorgang integrieren. Verwenden Sie einen EPI-Agent zum Ausführen von Visual Basic-Skripten als zusätzliche Schritte beim Bereitstellungsprozess.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- Überprüfen Sie, ob die Anforderungen in [Anforderungen für Visual Basic-Skripterstellung](#) erfüllt werden.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

6 Wählen Sie **Komponentenauswahl** auf der Seite für die Installationsarten aus.

7 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

8 Klicken Sie auf **Weiter**.

9 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie **EPIPowerShell** aus der Liste für den Agenttyp aus.

12 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

13 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

14 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

15 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

16 Wählen Sie den EPI-Typ aus.

17 Geben Sie den vollqualifizierten Domännennamen des verwalteten Servers in das Textfeld **EPI-Server** ein.

18 Klicken Sie auf **Hinzufügen**.

19 Klicken Sie auf **Weiter**.

20 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

21 Klicken Sie auf **Weiter**.

22 Klicken Sie auf **Beenden**.

23 Überprüfen Sie, ob die Installation erfolgreich war.

24 (Optional) Fügen Sie mehrere Agents mit unterschiedlichen Konfigurationen und einen Endpoint auf dasselbe System hinzu.

Installieren des WMI-Agents für WMI-Remoteanforderungen

Ein Systemadministrator aktiviert das WMI-Protokoll (Windows Management Instrumentation) und installiert den WMI-Agent auf allen verwalteten Windows-Maschinen, um die Verwaltung von Daten und Vorgängen zu aktivieren. Der Agent ist für das Erfassen von Daten von Windows-Maschinen erforderlich, wie beispielsweise der Active Directory-Status des Maschinenbesitzers.

Aktivieren von Remote-WMI-Anforderungen auf Windows-Maschinen

Für die Verwendung von WMI-Agents müssen Remote-WMI-Anforderungen auf den verwalteten Windows-Servern aktiviert sein.

Verfahren

- 1 Erstellen Sie in jeder Domäne, die bereitgestellte und verwaltete virtuelle Windows-Maschinen enthält, eine Active Directory-Gruppe und fügen Sie ihr die Anmeldedaten für Dienste der WMI-Agents hinzu, die Remote-WMI-Anforderungen auf den bereitgestellten Maschinen ausführen.
- 2 Aktivieren Sie auf jeder bereitgestellten Windows-Maschine Remote-WMI-Anforderungen für die Active Directory-Gruppen, die die Agent-Anmeldedaten enthalten.

Installieren des WMI-Agents

Der WMI-Agent (Windows Management Instrumentation) aktiviert die Datenerfassung von Windows-verwalteten Maschinen.

Voraussetzungen

- Installieren Sie IaaS, einschließlich Webserver und Manager Service-Host.
- Überprüfen Sie, ob die Anforderungen in [Aktivieren von Remote-WMI-Anforderungen auf Windows-Maschinen](#) erfüllt werden.
- [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#).

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 2 Klicken Sie auf **Weiter**.
- 3 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für die vRealize Automation-Appliance an und überprüfen Sie das SSL-Zertifikat.

a Geben Sie den Benutzernamen ein, der **root** lautet, sowie das Kennwort.

Das Kennwort ist das Kennwort, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

b Wählen Sie **Zertifikat akzeptieren** aus.

c Klicken Sie auf **Zertifikat anzeigen**.

Vergleichen Sie den Zertifikatfingerabdruck mit dem für die vRealize Automation-Appliance festgelegten Fingerabdruck. Sie können das Zertifikat für die vRealize Automation-Appliance im Client-Browser anzeigen, wenn auf die Verwaltungskonsole an Port 5480 zugegriffen wird.

5 Wählen Sie **Benutzerdefinierte Installation** auf der Seite für die Installationsarten aus.

6 Wählen Sie **Komponentenauswahl** auf der Seite für die Installationsarten aus.

7 Akzeptieren Sie den Stamminstallationsort oder klicken Sie auf **Ändern** und wählen Sie einen Installationspfad aus.

Selbst in einer verteilten Bereitstellung installieren Sie möglicherweise mehrere IaaS-Komponenten auf demselben Windows-Server.

Wenn Sie mehrere IaaS-Komponenten installieren, sollten Sie diese unbedingt im selben Pfad installieren.

8 Klicken Sie auf **Weiter**.

9 Melden Sie sich mit Administratorberechtigungen für die Windows-Dienste auf der Installationsmaschine an.

Der Dienst muss auf derselben Installationsmaschine ausgeführt werden.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie **WMI** aus der Liste **Agenttyp** aus.

12 Geben Sie einen Bezeichner für diesen Agent in das Textfeld **Agent-Name** ein.

Rufen Sie einen Datensatz des Agent-Namens, der Anmeldedaten, des Endpoint-Namens und der Plattform-Instanz für jeden Agent ab. Sie benötigen diese Informationen zum Konfigurieren von Endpoints und zum Hinzufügen von Hosts in der Zukunft.

Wichtig Für High Availability können Sie redundante Agents hinzufügen und sie identisch konfigurieren. Konfigurieren Sie die Agents andernfalls eindeutig.

Option	Beschreibung
Redundanter Agent	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
Eigenständiger Agent	Weisen Sie dem Agent einen eindeutigen Namen zu.

13 Konfigurieren Sie eine Verbindung zum IaaS Manager Service-Host.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein (<i>mgr-svc-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben (<i>mgr-svc.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

14 Konfigurieren Sie eine Verbindung zum IaaS-Webserver.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Webserver-Komponente installiert haben (<i>web.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.

Der Standardport lautet 443.

15 Klicken Sie auf **Testen** zum Überprüfen der Konnektivität für jeden Host.

16 Klicken Sie auf **Hinzufügen**.

17 Klicken Sie auf **Weiter**.

18 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Nach einigen Minuten wird eine Erfolgsmeldung angezeigt.

19 Klicken Sie auf **Weiter**.

20 Klicken Sie auf **Beenden**.

21 Überprüfen Sie, ob die Installation erfolgreich war.

22 (Optional) Fügen Sie mehrere Agents mit unterschiedlichen Konfigurationen und einen Endpoint auf dasselbe System hinzu.

Automatische Installation von vRealize Automation

vRealize Automation enthält Optionen für die skriptbasierte, automatische Installation über die Befehlszeile sowie Optionen für die API-basierte, unbeaufsichtigte Installation. Für beide Installationsmethoden ist es erforderlich, dass Sie im Voraus die Werte vorbereiten, die Sie normalerweise während einer herkömmlichen Installation von Hand eingeben würden.

Informationen zur automatischen Installation von vRealize Automation

Die automatische Installation von vRealize Automation verwendet eine ausführbare Datei, die auf eine textbasierte Antwortdatei verweist.

In der Antwortdatei nehmen Sie eine Vorkonfiguration der System-FQDNs, Kontoanmeldedaten und anderen Einstellungen vor, die Sie in der Regel in einer herkömmlichen auf einem Assistenten basierten oder manuellen Installation hinzufügen. Die automatische Installation ist bei folgenden Bereitstellungstypen nützlich:

- Bereitstellung mehrerer, nahezu identischer Umgebungen
- Wiederholte Bereitstellung derselben Umgebung
- Durchführen automatischer Installationen
- Durchführen von Skriptinstallationen

Ausführen einer automatischen vRealize Automation -Installation

Sie können eine automatische, unbeaufsichtigte vRealize Automation-Installation über die Konsole einer neu bereitgestellten vRealize Automation-Appliance ausführen.

Voraussetzungen

- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).
- Erstellen oder identifizieren Sie die IaaS-Windows-Server und konfigurieren Sie dazugehörige Voraussetzungen.
- Installieren Sie den Management-Agent auf den IaaS-Windows-Servern.

Sie können den Management-Agent unter Verwendung des herkömmlichen `.msi`-Dateidownloads oder des in [Ausführen einer automatischen Installation des vRealize Automation-Management-Agents](#) beschriebenen unbeaufsichtigten Vorgangs installieren.

Verfahren

- 1 Melden Sie sich bei der Konsole der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Navigieren Sie zum folgenden Verzeichnis.

```
/usr/lib/vcac/tools/install
```
- 3 Öffnen Sie die Antwortdatei `ha.properties` in einem Texteditor.
- 4 Fügen Sie für die Bereitstellung spezifische Einträge zur Datei `ha.properties` hinzu. Speichern und schließen Sie anschließend die Datei.

Schneller geht es, wenn Sie die Datei `ha.properties` aus einer anderen Bereitstellung kopieren und ändern, anstatt die gesamte Standarddatei zu bearbeiten.

- 5 Starten Sie über dasselbe Verzeichnis die Installation durch Ausführen des folgenden Befehls.

```
vra-ha-config.sh
```

Die Fertigstellung der Installation kann abhängig von der Umgebung und der Größe der Bereitstellung bis zu einer Stunde oder länger dauern.

- 6 (Optional) Überprüfen Sie nach Abschluss der Installation die Protokolldatei.

```
/var/log/vcac/vra-ha-config.log
```

Das Programm für die automatische Installation speichert keine proprietären Daten im Protokoll (wie beispielsweise Kennwörter, Lizenzen oder Zertifikate).

Ausführen einer automatischen Installation des vRealize Automation - Management-Agents

Sie können eine befehlszeilenbasierte Installation des vRealize Automation-Management-Agents auf jedem IaaS-Windows-Server ausführen.

Die automatische Installation des Management-Agents besteht aus einem Windows PowerShell-Skript, in dem Sie einige Einstellungen anpassen können. Nach dem Hinzufügen der bereitstellungsspezifischen Einstellungen können Sie die automatische Installation des Management-Agents auf allen IaaS-Windows-Servern durchführen, indem Sie auf jedem einzelnen Kopien desselben Skripts ausführen.

Voraussetzungen

- Erstellen Sie eine nicht konfigurierte Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).
- Erstellen oder identifizieren Sie die IaaS-Windows-Server und konfigurieren Sie dazugehörige Voraussetzungen.

Verfahren

- 1 Melden Sie sich auf dem IaaS-Windows-Server mit einem Konto mit Administratorrechten an.
- 2 Öffnen Sie die URL des Installationsprogramms für die vRealize Automation-Appliance in einem Webbrowser.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 3 Klicken Sie mit der rechten Maustaste auf die `InstallManagementAgent.ps1`-PowerShell-Skriptdatei und speichern Sie sie auf dem Desktop oder in einem Ordner auf dem IaaS-Windows-Server.
- 4 Öffnen Sie die Datei `InstallManagementAgent.ps1` in einem Texteditor.
- 5 Fügen Sie im oberen Bereich der Skriptdatei die bereitstellungsspezifischen Einstellungen hinzu.
 - Die URL der vRealize Automation-Appliance

```
https://vrealize-automation-appliance-FQDN:5480
```
 - Die Anmeldedaten für das Root-Benutzerkonto der vRealize Automation-Appliance

- Anmeldedaten für den vRealize Automation-Dienstbenutzer, ein Domänenkonto mit Administratorberechtigungen auf den IaaS-Windows-Servern
 - Der Ordner, in dem Sie den Management-Agent installieren möchten, standardmäßig Programme (x86)
 - (Optional) Der Fingerabdruck des Zertifikats im PEM-Format, das Sie für die Authentifizierung verwenden
- 6 Speichern und schließen Sie `InstallManagementAgent.ps1`.
 - 7 Doppelklicken Sie für eine automatische Installation des Management-Agents auf `InstallManagementAgent.ps1`.
 - 8 (Optional) Stellen Sie sicher, dass die Installation abgeschlossen ist, indem Sie **VMware vCloud Automation Center-Management-Agent** in der Liste der Programme und Funktionen in der Windows-Systemsteuerung sowie in der Liste der ausgeführten Windows-Dienste suchen.

Antwortdatei der unbeaufsichtigten vRealize Automation -Installation

Für die unbeaufsichtigte vRealize Automation-Installation ist die Vorbereitung einer textbasierten Antwortdatei im Vorfeld erforderlich.

Eine neu bereitgestellte vRealize Automation-Appliance enthält eine Standardantwortdatei.

```
/usr/lib/vcac/tools/install/ha.properties
```

Um eine unbeaufsichtigte Installation auszuführen, müssen Sie unter Verwendung eines Texteditors die Einstellungen in `ha.properties` an die zu installierende Bereitstellung anpassen. Die folgenden Beispiele sind nur einige der Einstellungen und Informationen, die Sie hinzufügen müssen.

- Der vRealize Automation- oder Suite-Lizenzschlüssel
- FQDNs der vRealize Automation-Appliance-Knoten
- Anmeldedaten für das vRealize Automation-Appliance-Root-Benutzerkonto
- IaaS-Windows-Server-FQDNs, die als Web-Knoten, Manager Service-Knoten usw. agieren
- Anmeldedaten für den vRealize Automation-Dienstbenutzer, ein Domänenkonto mit Administratorberechtigungen auf den IaaS-Windows-Servern
- FQDNs der Lastausgleichsdienste
- Parameter der SQL Server-Datenbank
- Proxy-Agent-Parameter für die Herstellung der Verbindung zu Virtualisierungsressourcen
- Die Information, ob das Programm für die unbeaufsichtigte Installation versuchen sollte, fehlende Voraussetzungen für IaaS-Windows-Server zu korrigieren

Das Programm für die unbeaufsichtigte Installation kann viele fehlende Windows-Voraussetzungen korrigieren. Einige Konfigurationsprobleme wie beispielsweise unzureichende CPU können jedoch nicht durch das Programm für die unbeaufsichtigte Installation geändert werden.

Um Zeit einzusparen, können Sie die Datei `ha.properties` wiederverwenden und ändern, die für eine andere Bereitstellung konfiguriert wurde. Es muss sich dabei um eine Bereitstellung handeln, bei der die Einstellungen ähnlich waren. Wenn Sie vRealize Automation über den Installationsassistenten installieren, erstellt der Assistent die Einstellungen in der Datei `ha.properties` und speichert sie in dieser Datei. Die Datei kann für die Wiederverwendung und Änderung bei der Durchführung einer unbeaufsichtigten Installation einer ähnlichen Bereitstellung hilfreich sein.

Der Assistent speichert keine proprietären Einstellungen in der Datei `ha.properties` (wie beispielsweise Kennwörter, Lizenzen oder Zertifikate).

Die vRealize Automation -Installationsbefehlszeile

vRealize Automation enthält eine konsolenbasierte Befehlszeilenschnittstelle für die Durchführung von Installationsanpassungen, die nach der Erstinstallation erforderlich sein können.

Die Befehlszeilenschnittstelle (Command Line Interface, CLI) kann Installations- und Konfigurationsaufgaben ausführen, die nach der Erstinstallation über die browserbasierte Schnittstelle nicht mehr verfügbar sind. Zu den CLI-Funktionen zählen die erneute Überprüfung der Voraussetzungen, die Installation von IaaS-Komponenten, die Installation von Zertifikaten oder die Festlegung des vRealize Automation-Hostnamens, auf den Benutzer in ihren Webbrowsern verweisen.

Die CLI ist außerdem nützlich für erfahrene Benutzer, die für bestimmte Vorgänge Skripts erstellen möchten. Einige CLI-Funktionen werden bei der automatischen Installation verwendet. Wenn Sie mit beiden Funktionen vertraut sind, können Sie Ihre Kenntnisse der Installationskripts für vRealize Automation vertiefen.

Grundlagen für die Installation von vRealize Automation über die Befehlszeile

Die Befehlszeilenschnittstelle für die vRealize Automation-Installation verfügt über Grundfunktionen der obersten Ebene.

Die Grundfunktionen sind das Anzeigen der vRealize Automation-Knoten-IDs, das Ausführen von Befehlen, das Berichten des Befehlsstatus und das Anzeigen der Hilfeinformationen. Geben Sie den folgenden Befehl ohne Optionen oder Bezeichner ein, um diese Vorgänge und die entsprechenden Optionen in der Konsolenansicht anzuzeigen.

```
vra-command
```

Anzeigen von Knoten-IDs

Sie benötigen vRealize Automation-Knoten-IDs, damit Sie für die richtigen Zielsysteme Befehle ausführen können. Geben Sie zum Anzeigen der Knoten-IDs den folgenden Befehl ein.

```
vra-command list-nodes
```

Notieren Sie die Knoten-IDs vor dem Ausführen von Befehlen auf bestimmten Maschinen.

Ausführen von Befehlen

Die meisten Befehlszeilenfunktionen umfassen das Ausführen eines Befehls für einen Knoten im vRealize Automation-Cluster. Verwenden Sie die folgende Syntax, um einen Befehl auszuführen.

```
vra-command execute --node Knoten-ID Befehlsname --Parametername Parameterwert
```

Wie in der vorherigen Syntax gezeigt, erfordern viele Befehle vom Benutzer ausgewählte Parameter und Parameterwerte.

Anzeigen des Befehlsstatus

Einige Befehle nehmen mehr Zeit in Anspruch als andere. Um den Fortschritt eines eingegebenen Befehls zu prüfen, geben Sie folgenden Befehl ein.

```
vra-command status
```

Der Statusbefehl ist insbesondere für die Überwachung einer Hintergrundinstallation hilfreich, die bei großen Bereitstellungsgrößen eine lange Zeit in Anspruch nehmen kann.

Anzeigen der Hilfe

Geben Sie den folgenden Befehl ein, um Hilfeinformationen für alle verfügbaren Befehle anzuzeigen.

```
vra-command help
```

Geben Sie den folgenden Befehl ein, um Hilfeinformationen für einen einzelnen Befehl anzuzeigen.

```
vra-command help Befehlsname
```

Befehlsnamen für die vRealize Automation -Installation

Über Befehle erhalten Sie Konsolenzugriff auf viele vRealize Automation-Installations- und -Konfigurationsaufgaben, die Sie nach der Erstinstallation durchführen können.

Mithilfe der verfügbaren Befehle können beispielsweise folgende Funktionen ausgeführt werden.

- Hinzufügen einer anderen vRealize Automation-Appliance zu einer vorhandenen Installation
- Festlegen des Hostnamens, auf den Benutzer in einem Webbrowser verweisen, wenn sie auf vRealize Automation zugreifen
- Erstellen der SQL Server-aaS-Datenbank
- Ausführen der Voraussetzungsprüfung für einenaaS-Windows-Server
- Importieren von Zertifikaten

Um eine vollständige Liste der verfügbaren vRealize Automation-Befehle anzuzeigen, melden Sie sich bei der Konsole der vRealize Automation-Appliance an und geben Sie den folgenden Befehl ein.

```
vra-command help
```

Die lange Liste der Befehlsnamen und Parameter ist nicht in einer separaten Dokumentation zu finden. Für eine effektive Nutzung der Liste ermitteln Sie zunächst einen Befehl, der von Interesse für Sie ist. Schränken Sie dann den gewünschten Bereich ein, indem Sie den folgenden Befehl eingeben.

```
vra-command help Befehlsname
```

Die vRealize Automation -Installations-API

Die vRealize Automation-REST-API zur Installation bietet Ihnen die Möglichkeit, rein softwarekontrollierte Installationen für vRealize Automation zu erstellen.

Die Installations-API erfordert eine JSON-formatierte Version derselben Einträge, die die CLI-basierte Installation aus der Answer-Datei der `ha.properties` bezieht. Die folgenden Richtlinien erläutern, wie die API funktioniert. Damit sollten Sie programmierte API-Aufrufe entwickeln können, um vRealize Automation zu installieren.

- Die API-Dokumentation finden Sie auf der folgenden Seite der vRealize Automation-Appliance.

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

Sie benötigen eine nicht konfigurierte vRealize Automation-Appliance. Siehe [Bereitstellen der vRealize Automation-Appliance](#).

- Um die API-basierte Installation auszuprobieren, suchen und erweitern Sie folgenden PUT-Befehl.

```
PUT /vra-install
```

- Kopieren Sie die nicht ausgefüllte JSON-Datei aus dem `install_json`-Feld in einen Texteditor. Tragen Sie die Answer-Werte so ein, wie Sie das in der Datei `ha.properties` tun würden. Wenn Sie die JSON-formatierten-Antworten eingetragen haben, kopieren Sie den Code zurück in die `install_json`-Datei und überschreiben Sie die nicht ausgefüllte JSON.

Sie können jedoch auch die folgende JSON-Vorlagendatei bearbeiten und das Ergebnis in die `install_json`-Datei kopieren.

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Sie können eine ausgefüllte `ha.properties`-Datei auch in JSON konvertieren oder umgekehrt.

- Wählen Sie im Aktionsfeld **Überprüfen** und klicken Sie auf **Ausprobieren**.

Damit wird die vRealize Automation-Voraussetzungsprüfung und Korrektur ausgeführt.

- Dabei wird eine alphanumerische Befehls-ID erstellt, die Sie in folgenden GET-Befehl einfügen können.

```
GET /commands/command-id/aggregated-status
```

In der Antwort des GET-Befehls finden Sie den Fortschritt der Überprüfung.

- Bei erfolgreicher Überprüfung können Sie die Installation ausführen, indem Sie das Verfahren wiederholen. Wählen Sie im Aktionsfeld einfach **Installieren** statt **Überprüfen**.

Je nach Bereitstellungsgröße kann die Installation längere Zeit in Anspruch nehmen. Suchen Sie die Befehls-ID und sehen Sie sich mithilfe des GET-Befehls den Installationsfortschritt an. Die GET-Antwort kann beispielsweise so aussehen:

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18, "queued": 3, "processing": 1}, "failed-commands": 0
```

- Wenn die Installation fehlschlägt können Sie mit folgenden Befehl eine Protokollerfassung für alle Knoten auslösen.

```
PUT /commands/log-bundle
```

Ähnlich wie bei der Installation wird eine alphanumerische Befehls-ID ausgegeben, mit der Sie die Protokollerfassung überwachen können.

Konvertierung von vRealize Automation -Eigenschaften der automatischen Installation in JSON

Bei CLI- oder API-basierten automatischen Installationen von vRealize Automation können Sie eine vollständige Answer-Datei der Eigenschaften in JSON konvertieren oder umgekehrt. Die automatische CLI-Installation erfordert die Eigenschaftendatei, während die API das JSON-Format erfordert.

Voraussetzungen

Eine vollständige Answer-Datei der Eigenschaften oder vollständige JSON-Datei

```
/usr/lib/vcac/tools/install/ha.properties
```

oder

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Verfahren

- 1 Melden Sie sich bei der Konsolensitzung der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Führen Sie das entsprechende Konverterskript aus.

- Konvertieren von JSON in Eigenschaften

```
/usr/lib/vcac/tools/install/convert-properties --from-json installationProperties.json
```

Das Skript erstellt eine neue Eigenschaftendatei mit Zeitstempel im Namen, z. B.:

```
ha.2016-10-17_13.02.15.properties
```

- Konvertieren von Eigenschaften in JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

Das Skript erstellt eine neue `installationProperties.json`-Datei mit Zeitstempel im Namen, z. B.:

```
installationProperties.2016-10-17_13.36.13.json
```

Sie können auch die Hilfe für das Skript anzeigen.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

vRealize Automation -Aufgaben nach der Installation

Nach der Installation von vRealize Automation müssen Sie sich möglicherweise um Aufgaben nach der Installation kümmern.

Konfigurieren der Federal Information Processing Standard-konformen Verschlüsselung

Sie können die mit Federal Information Processing Standard (FIPS) 140–2 konforme Verschlüsselung für eingehenden und ausgehenden Netzwerkverkehr der vRealize Automation-Appliance aktivieren oder deaktivieren.

Eine Änderung der FIPS-Einstellung erfordert einen Neustart von vRealize Automation. FIPS ist standardmäßig deaktiviert.

Verfahren

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

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

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

- 3 Klicken Sie oben rechts auf die Schaltfläche, um FIPS zu aktivieren oder zu deaktivieren.

Bei einer Aktivierung verwendet der eingehende und ausgehende Netzwerkverkehr der vRealize Automation-Appliance am Port 443 eine FIPS 140–2-konforme Verschlüsselung. Unabhängig von der FIPS-Einstellung verwendet vRealize Automation AES–256-konforme Algorithmen, um gesicherte Daten zu schützen, die auf der vRealize Automation-Appliance gespeichert sind.

Hinweis Diese vRealize Automation-Version ist nur teilweise FIPS-konform, da einige interne Komponenten noch keine zertifizierten Verschlüsselungsmodule verwenden. Wenn noch keine zertifizierten Module implementiert sind, werden die AES-256-konformen Algorithmen verwendet.

- 4 Klicken Sie auf **Ja**, um neu zu starten vRealize Automation.

Sie können FIPS auch in einer Konsolensitzung der vRealize Automation-Appliance als Root-Benutzer mit folgenden Befehlen konfigurieren.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Aktivieren des automatischen Manager Service-Failovers

Das automatische Manager Service-Failover ist standardmäßig deaktiviert, wenn Sie den Manager Service mit dem Windows-Standardinstallationsprogramm für vRealize Automation installieren.

Führen Sie zum Aktivieren des automatischen Manager Service-Failovers nach der Ausführung des standardmäßigen Windows-Installationsprogramms die folgenden Schritte aus.

Verfahren

1 Melden Sie sich als Root-Benutzer bei einer Konsolensitzung auf der vRealize Automation-Appliance an.

2 Navigieren Sie zum folgenden Verzeichnis.

```
/usr/lib/vcac/tools/vami/commands
```

3 Geben Sie den folgenden Befehl ein.

```
python ./manager-service-automatic-failover ENABLE
```

Wenn Sie das automatische Failover während einer IaaS-Bereitstellung deaktivieren müssen, geben Sie stattdessen den folgenden Befehl ein.

```
python ./manager-service-automatic-failover DISABLE
```

Informationen zum automatischen Manager Service-Failover

Sie können den vRealize Automation IaaS Manager Service so konfigurieren, dass ein Failover zu einem Backup durchgeführt wird, wenn der primäre Manager Service beendet wird.

Ab vRealize Automation 7.3 müssen Sie den Manager Service nicht mehr auf jedem Windows-Server manuell starten oder beenden, um zu steuern, welcher Server als primärer Server oder als Backup dient. Das automatische Manager Service-Failover ist in den folgenden Fällen standardmäßig aktiviert.

- Wenn Sie vRealize Automation mittels automatischer Installation oder mit dem Installationsassistenten installieren
- Wenn Sie ein Upgrade von IaaS über die Verwaltungsschnittstelle oder mit dem Skript für automatische Upgrades durchführen.

Failover ist nicht aktiviert, wenn Sie das standardmäßige Windows-basierte Installationsprogramm zum Hinzufügen eines Manager Service-Hosts oder IaaS-Upgrades verwenden. Informationen zur Failover-Aktivierung finden Sie unter [Aktivieren des automatischen Manager Service-Failovers](#).

Wenn automatisches Failover aktiviert ist, wird der Manager Service automatisch auf allen Manager Service-Hosts, einschließlich der Backups, gestartet. Die Funktion für automatisches Failover ermöglicht Hosts die transparente gegenseitige Überwachung und die Durchführung eines Failovers nach Bedarf. Zur Ausführung dieser Funktion muss der Windows-Dienst auf allen Hosts ausgeführt werden.

Hinweis Es ist nicht erforderlich, automatisches Failover zu verwenden. Sie können diese Funktion deaktivieren und den Windows-Dienst weiterhin manuell starten und beenden, um zu steuern, welcher Host als primärer Host oder als Backup dient. Beim manuellen Failover müssen Sie den Dienst nur jeweils auf einem Host starten. Bei deaktiviertem automatischem Failover führt die gleichzeitige Ausführung des Diensts auf mehreren IaaS-Servern dazu, dass vRealize Automation nicht mehr verwendet werden kann.

Versuchen Sie nicht, automatisches Failover selektiv zu aktivieren oder zu deaktivieren. Automatisches Failover muss immer auf jedem Manager Service-Host in einer IaaS-Bereitstellung als aktiviert oder deaktiviert synchronisiert werden.

Wenn das automatische Failover nicht zu funktionieren scheint, finden Sie unter [Das automatische Manager Service-Failover wird nicht aktiviert](#) Tipps zur Fehlerbehebung.

Automatisches Failover der PostgreSQL-Datenbank von vRealize Automation

In einer vRealize Automation-Bereitstellung mit Hochverfügbarkeit ermöglichen einige Konfigurationen das automatische Failover der integrierten PostgreSQL-Datenbank von vRealize Automation.

Automatisches Failover wird unter folgenden Bedingungen im Hintergrund aktiviert.

- Die Bereitstellung mit Hochverfügbarkeit enthält drei vRealize Automation-Appliances.
Automatisches Failover wird mit nur zwei Appliances nicht unterstützt.
- Die Datenbankreplikation wird in der vRealize Automation-Verwaltungsschnittstelle unter „vRA-Einstellungen“ > „Datenbank“ auf den synchronen Modus festgelegt.

In der Regel sollten Sie möglichst kein manuelles Failover durchführen, während das automatische Failover aktiviert ist. Bei einigen Problemen im Zusammenhang mit Knoten wird das automatische Failover jedoch möglicherweise nicht durchgeführt, obwohl es aktiviert ist. Überprüfen Sie in diesem Fall, ob Sie ein manuelles Failover durchführen müssen.

- 1 Warten Sie nach einem Ausfall des primären PostgreSQL-Datenbankknotens bis zu 5 Minuten, bis sich der restliche Cluster stabilisiert hat.
- 2 Öffnen Sie auf einem verbleibenden vRealize Automation-Appliance-Knoten in einem Browser die folgende URL.

`https://vrealize-automation-appliance-FQDN:5434/api/status`
- 3 Suchen Sie nach `manualFailoverNeeded`.
- 4 Wenn `manualFailoverNeeded` wahr ist, führen Sie ein manuelles Failover durch.

Weitere Informationen finden Sie unter [Durchführen eines manuellen Failovers der vRealize Automation-Appliance-Datenbank](#).

Ersetzen von selbstsignierten Zertifikaten mit von einer Zertifizierungsstelle bereitgestellten Zertifikaten

Wenn Sie vRealize Automation mit selbstsignierten Zertifikaten installiert haben, möchten Sie diese möglicherweise vor der Bereitstellung an die Produktion durch von einer Zertifizierungsstelle bereitgestellte Zertifikate ersetzen.

Weitere Informationen zum Aktualisieren von Zertifikaten finden Sie unter [Aktualisierung von vRealize Automation-Zertifikaten](#).

Ändern von Hostnamen und IP-Adressen

Behalten Sie die für vRealize Automation-Systeme geplanten Hostnamen, FQDNs und IP-Adressen möglichst bei. Einige Änderungen nach der Installation sind möglich, können sich aber kompliziert gestalten.

- Wenn Sie den Hostnamen der Windows-Maschine ändern, die die IaaS SQL Server-Datenbank hostet, finden Sie weitere Informationen unter [Konfigurieren der SQL-Datenbank für einen neuen Hostnamen](#).
- Beim Wiederherstellen von IaaS-Komponenten kann das Umbenennen eines Hosts den IaaS-Webhost, den Manager Service-Host oder den jeweiligen Lastausgleichsdienst betreffen. Stellen Sie diese Hosts oder Lastausgleichsdienste entsprechend den Anweisungen für die Sicherung und Wiederherstellung in *vRealize Suite* wieder her.

Informationen zum Ändern des Hostnamens oder der IP-Adresse einer vRealize Automation-Appliance finden Sie in den folgenden Abschnitten.

Ändern des Hostnamens der vRealize Automation -Appliance

Bei der Verwaltung einer Umgebung oder eines Netzwerks müssen Sie einer vRealize Automation-Appliance unter Umständen einen anderen Hostnamen zuweisen.

Wichtig Beim Umbenennen wird vRealize Automation für einige Minuten offline geschaltet.

Für eigenständige, Master- oder vRealize Automation-Replikat-Appliances gelten die gleichen Schritte.

Verfahren

- 1 Erstellen Sie in DNS einen zusätzlichen Datensatz mit dem Hostnamen des neuen Knotens. Entfernen Sie den vorhandenen DNS-Dateneintrag mit dem alten Hostnamen noch nicht.
- 2 Warten Sie, bis der DNS-Replizierungsvorgang und die Zonenverteilung erfolgt ist.
- 3 Melden Sie sich an der Befehlszeile der vRealize Automation-Appliance als Root-Benutzer an.
- 4 Führen Sie folgenden Befehl aus.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

Eine Zertifikatsdatei ist optional, es sei denn, der Hostname der alten Appliance wurde in einem Zertifikat verwendet. Wenn dies der Fall ist, stellen Sie ein aktualisiertes Zertifikat mit dem neuen Hostnamen zur Verfügung.

Wenn Sie eine Zertifikatsdatei angeben, importiert der Befehl zum Umbenennen auch das Zertifikat und gibt eine Zertifikats-ID zurück.

Eine Zertifikatsdatei muss im gleichen Format wie die Textausgabe des API-Befehls `/config/ssl/generate-certificate` vorliegen und den neuen DNS-Namen im zugehörigen SAN-Feld enthalten.

- 5 Warten Sie mindestens 15 Minuten, bis der Umbenennungsvorgang abgeschlossen ist. Die Befehlsaktionen dauern einige Minuten. Hinzu kommen mehrere Minuten für die erneute Registrierung des Diensts.
- 6 Wenn der Hostname der alten Appliance mit einem Lastausgleichsdienst in einer HA-Umgebung verwendet wurde, führen Sie eine Neukonfiguration des Lastausgleichsdiensts mit dem neuen Namen durch.
- 7 Entfernen Sie in DNS den vorhandenen DNS-Datensatz mit dem alten Hostnamen.

Treten beim Ändern eines Hostnamens Probleme auf, verwenden Sie stattdessen die separaten Verfahren aus der vRealize Automation 7.3-Dokumentation.

Ändern der IP-Adresse der vRealize Automation -Appliance

Bei der Wartung einer Umgebung oder eines Netzwerks müssen Sie einer vorhandenen vRealize Automation-Appliance möglicherweise eine andere IP-Adresse zuweisen.

Voraussetzungen

- Erstellen Sie vorsichtshalber Snapshots von vRealize Automation-Appliances und IaaS-Servern.
- Untersuchen Sie als Root-Benutzer in einer Konsolensitzung auf den vRealize Automation-Appliances die Einträge in der Datei `/etc/hosts`.

Suchen Sie nach Adresszuweisungen, die mit den neuen IP-Adressen kollidieren können, und nehmen Sie nach Bedarf Änderungen vor.

Wiederholen Sie diesen Vorgang auf allen IaaS-Servern für die `Windows\system32\drivers\etc\hosts`-Datei.

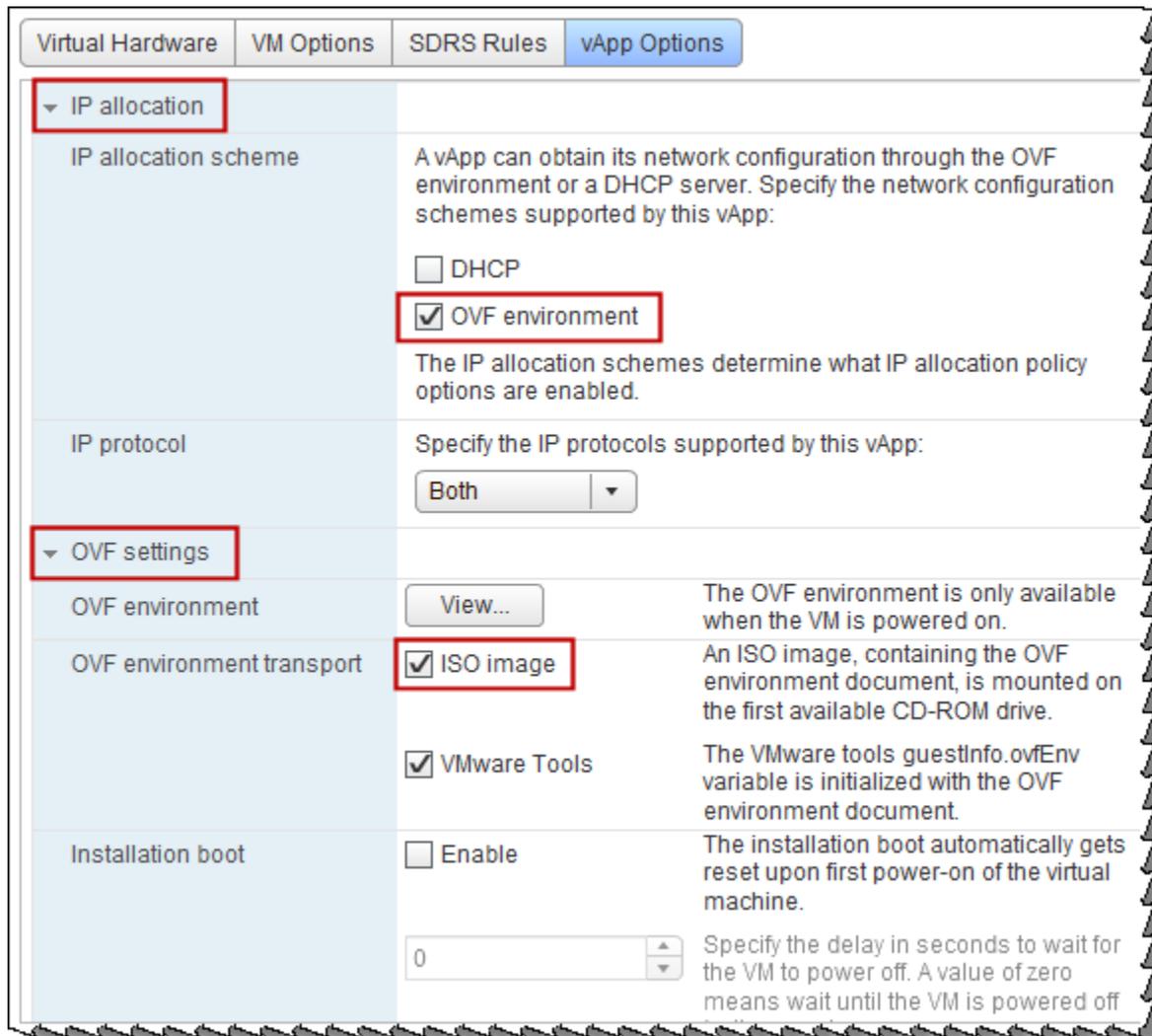
- Fahren Sie alle vRealize Automation-Appliances herunter.
- Beenden Sie sämtliche vRealize Automation-Dienste auf den IaaS-Servern.

Verfahren

- 1 Suchen Sie in vSphere die vRealize Automation-Appliance, die Sie ändern möchten, und wählen Sie **Aktionen > Einstellungen bearbeiten**.
- 2 Klicken Sie auf **vApp-Optionen**.
- 3 Erweitern Sie **IP-Zuteilung** und aktivieren Sie die Option **OVF-Umgebung**.

- Erweitern Sie **OVF-Einstellungen** und aktivieren Sie die Option **ISO-Image**.

Abbildung 1-16. OVF-Umgebung und ISO-Image-Optionen



- Klicken Sie auf **OK**.
- Starten Sie die vRealize Automation-Appliance, die Sie ändern.
- Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
<https://vrealize-automation-appliance-FQDN:5480>
- Klicken Sie auf die Registerkarte **Netzwerk**.
- Klicken Sie unter den Registerkarten auf **Adresse**.
- Aktualisieren Sie die IP-Adresse.
- Klicken Sie oben rechts auf **Einstellungen speichern**.
- Fahren Sie die vRealize Automation-Appliance herunter, die Sie ändern.

13 Aktualisieren Sie in DNS die Einträge für die neuen IP-Adressen.

Aktualisieren Sie nur vorhandene A-Typ-Datensätze. FQDNs sollten Sie nicht ändern.

Wenn Sie einen Lastausgleichsdienst verwenden, aktualisieren Sie nach Bedarf auch die IP-Einstellungen des Dienstes für Backend-Knoten, Dienst-Pools und virtuelle Server.

14 Warten Sie, bis der DNS-Replizierungsvorgang und die Zonenverteilung erfolgt ist.

15 Starten Sie alle vRealize Automation-Appliances.

16 Starten Sie die vRealize Automation-Dienste auf den IaaS-Servern.

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

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

18 Überprüfen Sie den vRealize Automation-Appliance-Status in den folgenden Bereichen.

- Datenbankverbindungsstatus unter **vRA-Einstellungen > Datenbank**
- RabbitMQ-Status unter **vRA-Einstellungen > Messaging**
- Xenon-Status unter **vRA-Einstellungen > Xenon**
- Alle Dienste als REGSTRIERT unter **Dienste**

Anpassen der SQL-Datenbank für einen geänderten Hostnamen

Wenn Sie die vRealize Automation IaaS SQL-Datenbank auf einen anderen Hostnamen verschieben, müssen Sie Konfigurationseinstellungen überarbeiten.

Sie können für denselben Hostnamen die SQL-Datenbank aus einer Sicherung wiederherstellen, ohne dass weitere Schritte erforderlich sind. Wenn Sie einen anderen Hostnamen wiederherstellen, müssen Sie Konfigurationsdateien bearbeiten, um weitere Änderungen vorzunehmen.

Erforderliche Änderungen beim Verschieben der SQL-Datenbank zu einem anderen Hostnamen finden Sie im [VMware-Knowledgebase-Artikel 2074607](#).

Ändern der IP-Adresse eines IaaS -Servers

Bei der Wartung einer Umgebung oder eines Netzwerks müssen Sie einem vorhandenen vRealize Automation-IaaS-Windows-Server möglicherweise eine andere IP-Adresse zuweisen.

Voraussetzungen

- Wenn die IP-Adresse der vRealize Automation-Appliance geändert werden muss, erledigen Sie dies zuerst. Siehe [Ändern der IP-Adresse der vRealize Automation-Appliance](#).
- Erstellen Sie vorsichtshalber Snapshots von vRealize Automation-Appliances und IaaS-Servern.
- Untersuchen Sie als Root-Benutzer in einer Konsolensitzung auf der vRealize Automation-Appliance die Einträge in der Datei `/etc/hosts`.

Suchen Sie nach Adresszuweisungen, die mit den neuen IP-Adressen kollidieren können, und nehmen Sie nach Bedarf Änderungen vor.

Wiederholen Sie diesen Vorgang auf allen IaaS-Servern für die `Windows\system32\drivers\etc\hosts`-Datei.

- Fahren Sie die vRealize Automation-Appliance herunter.
- Beenden Sie sämtliche vRealize Automation-Dienste auf den IaaS-Servern.

Verfahren

- 1 Melden Sie sich auf dem IaaS-Server mit einem Konto mit Administratorrechten an.
- 2 Ändern Sie in Windows die IP-Adresse.

Suchen Sie in den Netzwerkkadptereinstellungen von Windows unter Internetprotokolleigenschaften nach der IP-Adresse.

- 3 Aktualisieren Sie Ihren lokalen DNS-Server mit den Änderungen.

Durch das Aktualisieren von DNS wird sichergestellt, dass die IaaS-Windows-Server einander finden und dass Sie sich mit einem Windows-Server erneut verbinden können, wenn die Verbindung getrennt wurde.

- 4 Überprüfen Sie auf dem Manager-Dienst-Host die folgende Datei in einem Texteditor:

`Installationsordner\VCAC\Server\ManagerService.exe.config`

Der Standardinstallationsordner lautet `C:\Programme (x86)\VMware`.

Überprüfen Sie die IP-Adressen oder FQDNs der vRealize Automation-Appliances und IaaS-Windows-Server.

- 5 Überprüfen Sie auf allen IaaS-Windows-Servern die folgende Datei in einem Texteditor:

`Installationsordner\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

Überprüfen Sie die IP-Adresse oder den FQDN der vRealize Automation-Appliance.

- 6 Melden Sie sich beim SQL Server-Host an.
- 7 Stellen Sie sicher, dass die Repository-Adresse korrekt für die Verwendung von FQDN in der Spalte „ConnectionString“ konfiguriert ist.

Öffnen Sie beispielsweise SQL Management Studio und führen Sie die folgende Abfrage aus:

```
"SELECT Name, ConnectionString FROM [Datenbankname].[DynamicOps.RepositoryModel].[Models]"
```

- 8 Starten Sie die vRealize Automation-Appliance.
- 9 Starten Sie die vRealize Automation-Dienste auf den IaaS-Servern.
- 10 Überprüfen Sie die Protokolldateien, um sicherzustellen, dass der Agent-Dienst, der DEM-Worker-Dienst, der Manager-Dienst und Web-Host-Dienste erfolgreich gestartet wurden.
- 11 Melden Sie sich bei vRealize Automation als Benutzer mit der Infrastrukturadministratorrolle an.

- 12 Navigieren Sie zu **Infrastruktur > Überwachung > Status verteilte Ausführung** und stellen Sie sicher, dass alle Dienste ausgeführt werden.
- 13 Testen Sie auf einen ordnungsgemäßen Betrieb, indem Sie die Appliance-Dienste überprüfen, die Bereitstellung testen oder das vRealize Production Test-Tool verwenden.

Ändern eines IaaS -Server-Hostnamens

Bei der Wartung einer Umgebung oder eines Netzwerks müssen Sie einem vorhandenen vRealize Automation-IaaS-Windows-Server möglicherweise einen anderen Hostnamen zuweisen.

Verfahren

- 1 Erstellen Sie einen Snapshot des IaaS-Servers.
- 2 Verwenden Sie auf dem IaaS-Server IIS-Manager, um die vRealize Automation-Anwendungspools Repository, VMware vRealize Automation-Repository und Wapi zu beenden.
- 3 Verwenden Sie auf dem IaaS-Server „Verwaltungstools > Services“, um alle vRealize Automation-Services, -Agents und -DEMs zu beenden.
- 4 Erstellen Sie in DNS einen zusätzlichen Dateneintrag mit dem neuen Hostnamen.
Entfernen Sie den vorhandenen DNS-Dateneintrag mit dem alten Master-Hostnamen noch nicht.
- 5 Warten Sie, bis der DNS-Replizierungsvorgang und die Zonenverteilung erfolgt ist.
- 6 Ändern Sie auf dem IaaS-Server den Hostnamen, starten Sie jedoch bei Aufforderung nicht neu.
Suchen Sie den Hostnamen in den Windows-Systemeigenschaften unter den Einstellungen für Computernamen, Domäne und Arbeitsgruppe.
Wenn Sie zum Neustart aufgefordert werden, klicken Sie auf die Option für einen späteren Neustart.
- 7 Wenn Sie den alten Hostnamen verwendet haben, um Zertifikate zu generieren, aktualisieren Sie die Zertifikate.
Weitere Informationen finden Sie unter [Aktualisieren von vRealize Automation-Zertifikaten](#).
- 8 Verwenden Sie einen Texteditor, um den Hostnamen in Konfigurationsdateien zu suchen und zu aktualisieren.
Nehmen Sie die Aktualisierungen in Abhängigkeit davon vor, welchen IaaS-Server-Hostnamen Sie geändert haben. In einer verteilten HA-Bereitstellung müssen Sie möglicherweise auf mehr als einen Server zugreifen. Es sind keine Updates vorhanden, wenn Sie den Hostnamen eines DEM-Orchestrators oder DEM-Workers ändern.

Hinweis Aktualisieren Sie nur den alten Windows-Server-Hostnamen. Wenn Sie stattdessen den Namen eines Lastausgleichsdiensts finden, behalten Sie diesen Namen bei.

Tabelle 1-40. Dateien, die aktualisiert werden müssen, wenn Sie den Hostnamen eines Web-Knotens ändern

laaS-Server	Pfad	Datei
Web-Knoten	<i>Installationsordner\Server\Website</i>	Web.config
	<i>Installationsordner\Server\Website\Cafe</i>	Vcac-Config.exe.config
	<i>Installationsordner\Web API</i>	Web.config
	<i>Installationsordner\Web API\ConfigTool</i>	Vcac-Config.exe.config
Knoten mit installierter Model Manager-Komponente	<i>Installationsordner\Server\Model Manager Data</i>	Reputil.exe.config
	<i>Installationsordner\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Manager Service-Knoten	<i>Installationsordner\Server</i>	ManagerService.exe.config
DEM-Orchestrator-Knoten	<i>Installationsordner\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
DEM-Worker-Knoten	<i>Installationsordner\Distributed Execution Manager\DEM-Name</i>	DynamicOps.DEM.exe.config
Agent-Knoten	<i>Installationsordner\Agents\Agent-Name</i>	RepoUtil.exe.config
	<i>Installationsordner\Agents\Agent-Name</i>	VRMAgent.exe.config

Tabelle 1-41. Dateien, die aktualisiert werden müssen, wenn Sie den Hostnamen eines Manager Service-Knotens ändern

laaS-Server	Pfad	Datei
DEM-Orchestrator-Knoten	<i>Installationsordner\Distributed Execution Manager\DEM-Name</i>	DynamicOps.DEM.exe.config
DEM-Worker-Knoten	<i>Installationsordner\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Agent-Knoten	<i>Installationsordner\Agents\Agent-Name</i>	VRMAgent.exe.config

Tabelle 1-42. Dateien, die aktualisiert werden müssen, wenn Sie den Hostnamen eines Agent-Knotens ändern

laaS-Server	Pfad	Datei
Agent-Knoten	<i>Installationsordner\Agents\Agent-Name</i>	VRMAgent.exe.config

- 9 Starten Sie den laaS-Server neu, bei dem Sie den Hostnamen geändert haben.
- 10 Starten Sie die vRealize Automation-Anwendungspools, die Sie zuvor angehalten haben.
- 11 Starten Sie die vRealize Automation-Dienste, -Agents und -DEMs, die Sie zuvor angehalten haben.
- 12 Wenn der Hostname des alten laaS-Servers mit einem Lastausgleichsdienst in einer HA-Umgebung verwendet wurde, führen Sie eine Neukonfiguration des Lastausgleichsdiensts mit dem neuen Namen durch.
- 13 Entfernen Sie bei DNS den vorhandenen DNS-Eintrag mit dem alten Hostnamen.

- 14 Warten Sie, bis der DNS-Replizierungsvorgang und die Zonenverteilung erfolgt ist.
- 15 Wenn Sie den Hostnamen eines Manager Service-Hosts geändert haben, führen Sie die folgenden zusätzlichen Schritte durch.
 - a Aktualisieren Sie Software-Agents auf vorhandenen virtuellen Maschinen.
 - b Erstellen Sie alle ISOs oder Vorlagen neu, die einen Gast-Agent enthalten.

Nächste Schritte

Stellen Sie sicher, dass vRealize Automation einsatzbereit ist. Informationen dazu finden Sie in der Dokumentation [Sicherung und Wiederherstellung in vRealize Suite](#).

Festlegen der vRealize Automation -Anmelde-URL auf einen benutzerdefinierten Namen

Wenn sich vRealize Automation-Benutzer mit einem URL-Namen anmelden sollen, bei dem es sich nicht um den Namen der vRealize Automation-Appliance oder des Lastausgleichsdiensts handelt, müssen Sie vor und nach der Installation Anpassungen vornehmen.

Verfahren

- 1 Bereiten Sie vor der Installation ein Zertifikat vor, das den gewünschten CNAME-Eintrag sowie die Namen der vRealize Automation-Appliance und des Lastausgleichsdiensts enthält.
- 2 Installieren Sie vRealize Automation und geben Sie den Namen der Appliance oder des Lastausgleichsdiensts wie gewohnt ein. Importieren Sie das angepasste Zertifikat während der Installation.
- 3 Erstellen Sie nach der Installation im DNS einen aus einem allgemeinen Namen bestehenden CNAME-Alias und zeigen Sie auf die VIP-Adresse der Appliance oder des Lastausgleichsdiensts.
- 4 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.

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

- 5 Ändern Sie unter **vRA-Einstellungen > Hosteinstellungen** den **Hostnamen** in den ausgewählten CNAME-Eintrag.

Lizenzierung von vRealize Code Stream

Sie können vRealize Code Stream aktivieren, indem Sie eine vRealize Code Stream-Lizenz in vRealize Automation eingeben.

Sie können die vRealize Code Stream-Lizenz in einem der folgenden Speicherorte eingeben:

- Auf der Lizenzierungsseite des vRealize Automation-Installationsassistenten. Weitere Informationen finden Sie unter [vRealize Code Stream-Installation](#).
- Auf der Registerkarte „Lizenzierung“ in der Verwaltungsschnittstelle der vRealize Automation-Appliance. Weitere Informationen finden Sie unter [Anwenden einer vRealize Code Stream-Lizenz auf eine Appliance](#).

Installieren des vRealize Log Insight -Agents auf IaaS -Servern

Der vRealize Log Insight-Agent ist nicht standardmäßig auf den Windows-Servern in einer vRealize Automation IaaS-Konfiguration enthalten.

vRealize Log Insight bietet Protokoll-Aggregation und Indexerstellung und ermöglicht Ihnen das Erfassen, Importieren und Analysieren von Protokollen zur Aufdeckung von Systemproblemen. Wenn Sie Protokolle von IaaS-Servern mithilfe von vRealize Log Insight erfassen und analysieren möchten, müssen Sie den vRealize Log Insight-Agent für Windows getrennt installieren.

Weitere Informationen finden Sie in der [Dokumentation zu VMware vRealize Log Insight](#).

vRealize Automation-Appliances enthalten den vRealize Log Insight-Agent standardmäßig.

Ändern des VMware Remote Console-Proxy-Ports

Wenn Ihre Site Port 8444 blockiert oder anderweitig reserviert, können Sie den von VMware Remote Console verwendeten Standard-Proxy-Port ändern.

Verfahren

- 1 Melden Sie sich über die Eingabeaufforderung als Root-Benutzer bei der vRealize Automation-Appliance an.
- 2 Öffnen Sie die folgende Datei in einem Texteditor.
`/etc/vcac/security.properties`
- 3 Ändern Sie `consoleproxy.service.port` von seinem Standardwert 8444 in einen nicht verwendeten Port.
- 4 Speichern und schließen Sie `security.properties`.
- 5 Starten Sie die vRealize Automation-Appliance neu.

Nehmen Sie in einer HA-Umgebung dieselbe Änderung an allen vRealize Automation-Appliances vor.

Ändern eines vRealize Automation -Appliance-FQDN in den ursprünglichen FQDN

In einigen Fällen wird möglicherweise ein vRealize Automation-Appliance-FQDN geändert, obwohl Sie dies gar nicht möchten. Beispielsweise ändert sich der FQDN, wenn Sie ein IWA-Verzeichnis (Integrierte Windows-Authentifizierung) für eine Domäne erstellen, die nicht diejenige Domäne darstellt, auf der sich die Appliance befindet.

Wenn Sie ein IWA-Verzeichnis für eine andere Domäne erstellen, befolgen Sie die folgenden Schritte, um den Appliance-FQDN wieder in den ursprünglichen FQDN zu ändern.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an und erstellen Sie das IWA-Verzeichnis wie gewohnt.
Informationen finden Sie unter [Konfigurieren eines Active Directory über LDAP/IWA-Links](#).

- 2 Wenn es sich um eine HA-Umgebung handelt, befolgen Sie auch die Schritte unter [Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren](#).

- 3 Bei der Erstellung eines IWA-Verzeichnisses für eine Domäne, die nicht diejenige Domäne darstellt, auf der sich die Appliance befindet, wird der Appliance-FQDN ohne Benachrichtigung geändert.

Beispielsweise ändert sich va1.domain1.local in va1.domain2.local, wenn Sie ein IWA-Verzeichnis für domain2.local erstellen.

Machen Sie die Änderung rückgängig, indem Sie jede Appliance wieder in ihren ursprünglichen FQDN umbenennen. Die entsprechende Vorgehensweise finden Sie unter [Ändern von Hostnamen und IP-Adressen](#).

- 4 Nachdem die Appliances mit ihrem ursprünglichen FQDN wieder vollständig online sind, melden Sie sich bei jedem IaaS-Knoten an und führen Sie die folgenden Schritte aus.

- a Öffnen Sie die folgende Datei in einem Texteditor.

```
C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config
```

- b Ändern Sie jeden Appliance-endpoint address=-FQDN wieder in den ursprünglichen FQDN.

Beispiel: Von:

```
<endpoint address="https://va1.domain2.local:5480/" thumbprint="90C55BA-
EC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/" thumb-
print="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

In:

```
<endpoint address="https://va1.domain1.local:5480/" thumbprint="90C55BA-
EC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/" thumb-
print="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

- c Speichern und schließen Sie VMware.IaaS.Management.Agent.exe.Config.

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

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

- 6 Wechseln Sie zu **vRA-Einstellungen > Messaging** und klicken Sie auf **RabbitMQ-Cluster zurücksetzen**.

- 7 Melden Sie sich nach dem Zurücksetzen bei jeder Appliance-Verwaltungsschnittstelle an.

- 8 Wechseln Sie zu **vRA-Einstellungen > Cluster** und stellen Sie sicher, dass alle Knoten mit dem Cluster verbunden sind.

Konfigurieren von SQL AlwaysOn Availability Group

Sie müssen Konfigurationsänderungen vornehmen, wenn Sie nach der Installation von vRealize Automation SQL AlwaysOn Availability Group (AAG) einrichten.

Befolgen Sie beim Einrichten von SQL AAG nach der Installation die Schritte im [VMware-Knowledgebase-Artikel 2074607](#), um vRealize Automation mit dem AAG-Listener-FQDN als SQL Server-Host zu konfigurieren.

Hinzufügen von Netzwerkkarten nach der Installation von vRealize Automation

vRealize Automation unterstützt mehrere Netzwerkkarten (NICs). Nach der Installation können Sie Netzwerkkarten zur vRealize Automation-Appliance oder zum IaaS-Windows-Server hinzufügen.

Für einige vRealize Automation-Bereitstellungen sind möglicherweise mehrere Netzwerkkarten erforderlich, beispielsweise:

- Sie möchten Benutzer- und Infrastrukturnetzwerke trennen.
- Sie benötigen eine zusätzliche Netzwerkkarte, damit IaaS-Server einer Active Directory-Domäne beitreten können.

Weitere Informationen zu Szenarien mit mehreren Netzwerkkarten finden Sie in diesem [Blogbeitrag zum VMware Cloud Management](#).

Berücksichtigen Sie bei drei oder mehr Netzwerkkarten die folgenden Einschränkungen.

- VIDM benötigt Zugriff auf die Postgres-Datenbank und Active Directory.
- In einem HA-Cluster benötigt VIDM Zugriff auf die Lastausgleichsdienst-URL.
- Die vorangehenden VIDM-Verbindungen müssen über die ersten beiden Netzwerkkarten erfolgen.
- Netzwerkkarten nach der zweiten NIC dürfen nicht von VIDM verwendet oder erkannt werden.
- Netzwerkkarten nach der zweiten NIC dürfen nicht für die Verbindung mit Active Directory verwendet werden.

Verwenden Sie die erste oder zweite Netzwerkkarte, wenn Sie ein Verzeichnis in vRealize Automation konfigurieren.

Voraussetzungen

Installieren Sie vRealize Automation vollständig in Ihrer vCenter-Umgebung.

Verfahren

- 1 Fügen Sie in vCenter Netzwerkkarten für jede vRealize Automation-Appliance hinzu.
 - a Klicken Sie mit der rechten Maustaste auf die Appliance und wählen Sie **Einstellungen bearbeiten** aus.
 - b Fügen Sie VMXNETn-Netzwerkkarten hinzu.
 - c Wenn die Appliance eingeschaltet ist, starten Sie sie neu.

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

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

- 3 Wählen Sie **Netzwerk** aus und stellen Sie sicher, dass mehrere Netzwerkkarten verfügbar sind.
- 4 Wählen Sie die **Adresse** aus, und konfigurieren Sie die IP-Adresse für die Netzwerkkarten.

Tabelle 1-43. Beispiel für NIC-Konfiguration

Einstellung	Wert
IPv4-Adresstyp	Statisch
IPv4-Adresse	172.22.0.2
Netzmaske	255.255.255.0

- 5 Stellen Sie sicher, dass alle vRealize Automation-Knoten sich gegenseitig über DNS-Namen auflösen können.
- 6 Stellen Sie sicher, dass alle vRealize Automation-Knoten auf alle Lastausgleich-FQDNs für vRealize Automation-Komponenten zugreifen können.
- 7 Wenn Sie Split-Brain-DNS verwenden, stellen Sie sicher, dass alle vRealize Automation-Knoten und VIPs denselben FQDN in DNS für jede Knoten-IP und -VIP aufweisen.
- 8 Fügen Sie in vCenter Netzwerkkarten zu IaaS-Windows-Servern hinzu.
 - a Klicken Sie mit der rechten Maustaste auf den IaaS-Server und wählen Sie **Einstellungen bearbeiten** aus.
 - b Fügen Sie Netzwerkkarten zur virtuellen Maschine des IaaS-Servers hinzu.
- 9 Konfigurieren Sie in Windows die hinzugefügten IaaS-Server-NICs und deren IP-Adressen. Falls erforderlich, finden Sie weitere Informationen in der Microsoft-Dokumentation.

Nächste Schritte

(Optional) Wenn Sie statische Routen benötigen, finden Sie weitere Informationen unter [Konfigurieren von statischen Routen](#).

Konfigurieren von statischen Routen

Wenn Sie Netzwerkkarten zu einer vRealize Automation-Installation hinzufügen und statische Routen benötigen, öffnen Sie eine Eingabeaufforderungssitzung, um diese zu konfigurieren.

Voraussetzungen

Fügen Sie mehrere Netzwerkkarten zu vRealize Automation-Appliances oder IaaS-Windows-Servern hinzu.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Öffnen Sie die Routendatei in einem Texteditor.

```
/etc/sysconfig/network/routes
```

- 3 Suchen Sie die Zeile `default` für das Standard-Gateway, ändern Sie diese aber nicht.

Hinweis Verwenden Sie in Fällen, in denen das Standard-Gateway geändert werden muss, stattdessen die vRealize Automation-Verwaltungsschnittstelle.

- 4 Fügen Sie unterhalb der Zeile `default` neue Zeilen für statische Routen hinzu. Beispiel:

```
default 10.10.10.1 - -  
172.30.30.0 192.168.100.1 255.255.255.0 eth0  
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Speichern und schließen Sie die Routendatei.
- 6 Starten Sie die Appliance neu.
- 7 Wiederholen Sie den Vorgang in HA-Clustern für jede Appliance.
- 8 Melden Sie sich als Administrator beim IaaS-Windows-Server an.
- 9 Öffnen Sie eine Eingabeaufforderung als Administrator.
- 10 Um eine statische Route zu konfigurieren, geben Sie den Befehl `route -p add` ein, wobei `-p` die statische Route bei Neustarts persistiert. Beispiel:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1  
OK!
```

Weitere Informationen zur Konfiguration von statischen Routen in Windows finden Sie in der Microsoft-Dokumentation.

Zugriff auf Patch-Verwaltung

Technischer Support für Ihre vRealize Automation-Installation beinhaltet möglicherweise einen Software-Patch, den Sie mit der Verwaltungsschnittstelle der vRealize Automation-Appliance installieren oder entfernen.

Die Patch-Schnittstelle kann keine Patches auf die folgenden vRealize Automation-Komponenten anwenden.

- Management Agent
- Andere Agents als vSphere-Agents, wie XenServer, VDI oder Hyper-V

Voraussetzungen

- Erstellen Sie Snapshots von allen Knoten in Ihrer vRealize Automation-Installation.
- Stellen Sie sicher, dass alle Knoten in der vRealize Automation-Installation aktiv hochgefahren sind und ausgeführt werden.

Wenn Sie versuchen, einen Patch zu installieren oder zu entfernen, ohne dass alle Knoten ausgeführt werden, kann es passieren, dass die Verwaltungsschnittstelle der vRealize Automation-Appliance nicht mehr reagiert. Wenden Sie sich in diesem Fall an den technischen Support. Versuchen Sie nicht, Patches mit anderen Mitteln zu verwalten oder vRealize Automation zu verwenden, bis Sie das Problem behoben haben.

- Wenn Ihre Umgebung Lastausgleichsdienste für HA verwendet, deaktivieren Sie Datenverkehr zu sekundären Knoten, bis Patches installiert oder entfernt wurden.
- Wenn Sie einen neuen Patch installieren, rufen Sie die Patchdatei ab und kopieren Sie sie in das Dateisystem, das für den Browser verfügbar ist, mit dem Sie die Verwaltungsschnittstelle der vRealize Automation-Appliance verwenden.
- Die neuesten Patches oder neu veröffentlichte Informationen zu Patches finden Sie hier: [VMware-Knowledgebase](#).

Öffnen Sie die Knowledgebase und geben Sie *vRealize Automation patching* in das Suchfeld ein. Beispielsweise wird der [Artikel 51708 der VMware-Knowledgebase](#) überwacht und mit den neuesten vRealize Automation 7.4-Patch-Informationen aktualisiert.

Verfahren

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

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

- 2 Klicken Sie auf **vRA-Einstellungen > Patches**.
- 3 Klicken Sie unter der Patch-Verwaltung auf die gewünschte Option und folgen Sie den Eingabeaufforderungen.

Option	Beschreibung
Neuer Patch	Installieren Sie einen neuen Patch, den Sie heruntergeladen haben.
Installierte Patches	Fügen Sie den zuletzt installierten Patch zu neu hinzugefügten Clusterknoten hinzu.

Option	Beschreibung
Rollback	Entfernen Sie den zuletzt installierten Patch und setzen Sie vRealize Automation auf die vorherige Patch-Ebene zurück.
Verlauf	Überprüfen Sie die Liste der installierten und entfernten Patches.

Zum Aktivieren oder Deaktivieren der Patch-Verwaltung melden Sie sich bei der Eingabeaufforderung der vRealize Automation-Appliance als Root-Benutzer an und geben einen der folgenden Befehle ein.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Installieren eines neuen Patches

Sie installieren neue vRealize Automation-Patches über die Verwaltungsschnittstelle der vRealize Automation-Appliance.

Voraussetzungen

Prüfen Sie die Voraussetzungen und öffnen Sie die Patch-Verwaltungsschnittstelle. Siehe [Zugriff auf Patch-Verwaltung](#).

Verfahren

- 1 Klicken Sie auf **Neuer Patch**.
- 2 Klicken Sie auf **Patch hochladen**.
- 3 Suchen und wählen Sie die Patchdatei aus.
- 4 Überprüfen Sie nach dem Hochladen des Patches die Patchdetails.
- 5 Wenn Sie über den falschen Patch verfügen, brechen Sie den Vorgang ab, indem Sie auf **Entfernen** klicken. Klicken Sie andernfalls auf **Installieren**.
- 6 Vergewissern Sie sich, dass Sie die Voraussetzungen erfüllt haben, und klicken Sie auf **Installieren**. Das Installieren des Patches kann einige Minuten dauern.
- 7 Klicken Sie auf **Fertig**.

Wenn die Patchinstallation fehlschlägt, können Sie für einen erneuten Versuch auf **Wiederholen** klicken. Wählen Sie **Entfernen** aus, um den Vorgang abubrechen. Beim Abbrechen wird vRealize Automation auf den Status vor Beginn der Patchinstallation zurückgesetzt.

Installieren des aktuellen Patches auf neuen Knoten

Sie können den zuletzt installierten vRealize Automation-Patch zu neu hinzugefügten Clusterknoten hinzufügen.

Voraussetzungen

Prüfen Sie die Voraussetzungen und öffnen Sie die Patch-Verwaltungsschnittstelle. Siehe [Zugriff auf Patch-Verwaltung](#).

Verfahren

- 1 Klicken Sie auf **Installierte Patches**.
- 2 Wählen Sie den neuesten Patch aus.
- 3 Klicken Sie auf **Installieren**.
- 4 Folgen Sie den Anweisungen am Bildschirm.

Entfernen des aktuellen Patches

Sie können den zuletzt installierten vRealize Automation-Patch entfernen und ein Rollback auf den vorherigen Patch durchführen.

Voraussetzungen

Navigieren Sie zur Patch-Verwaltungsschnittstelle. Siehe [Zugriff auf Patch-Verwaltung](#).

Verfahren

- 1 Klicken Sie auf **Rollback**.
- 2 Wählen Sie den neuesten Patch aus.
- 3 Klicken Sie auf **Rollback**.
- 4 Folgen Sie den Anweisungen am Bildschirm.

Konfigurieren des Zugriffs auf den Standardmandanten

Sie müssen Ihren Team-Mitgliedern Zugriffsrechte auf den Standardmandanten erteilen, damit sie mit der Konfiguration von vRealize Automation beginnen können.

Der Standardmandant wird automatisch erstellt, wenn Sie Single Sign-On im Installationsassistenten konfigurieren. Sie können die Mandantendetails wie z. B. den Namen oder das URL-Token nicht bearbeiten, aber Sie können jederzeit neue lokale Benutzer erstellen und zusätzliche Mandanten- oder IaaS-Administratoren bestimmen.

Verfahren

- 1 Melden Sie sich bei vRealize Automation als Administrator des Standardmandanten an.
 - a Navigieren Sie zur vRealize Automation-Produktschnittstelle.
`https://vrealize-automation-FQDN/vcac`
 - b Melden Sie sich mit dem Benutzernamen **administrator** und dem Kennwort, das Sie für diesen Benutzer bei der Konfiguration von SSO definiert haben, an.
- 2 Wählen Sie **Administration > Mandanten** aus.
- 3 Klicken Sie auf den Namen des Standardmandanten, **vsphere.local**.
- 4 Klicken Sie auf die Registerkarte **Lokale Benutzer**.

5 Erstellen Sie lokale Benutzerkonten für den vRealize Automation-Standardmandanten.

Lokale Benutzer sind mandantenspezifisch und können nur auf den Mandanten zugreifen, in dem sie erstellt wurden.

- a Klicken Sie auf das Symbol „Hinzufügen“ (+).
- b Geben Sie für den Benutzer, der für die Verwaltung Ihrer Infrastruktur verantwortlich ist, Details ein.
- c Klicken Sie auf **Hinzufügen**.
- d Wiederholen Sie diesen Schritt, um einen oder mehrere zusätzliche Benutzer hinzuzufügen, die für die Konfiguration des Standardmandanten verantwortlich sein sollen.

6 Klicken Sie auf die Registerkarte **Administratoren.**

7 Weisen Sie Ihren lokalen Benutzern die Mandantenadministrator- und IaaS-Administratorrollen zu.

- a Geben Sie in das Suchfeld **Mandantenadministratoren** einen Benutzernamen ein und drücken Sie die Eingabetaste.
- b Geben Sie in das Suchfeld **IaaS-Administratoren** einen Benutzernamen ein und drücken Sie die Eingabetaste.

Der IaaS-Administrator ist für das Erstellen und Verwalten Ihrer Infrastruktur-Endpoints in vRealize Automation verantwortlich. Nur der Systemadministrator kann diese Rolle zuweisen.

8 Klicken Sie auf **Aktualisieren.**

Nächste Schritte

Stellen Sie Ihren Team-Mitgliedern die Zugriffs-URL und die Anmeldeinformationen für die erstellten Benutzerkonten zur Verfügung, sodass sie mit der Konfiguration von vRealize Automation beginnen können.

- Ihre Mandantenadministratoren konfigurieren Einstellungen wie z. B. die Benutzerauthentifizierung, einschließlich der Konfiguration der Verzeichnisverwaltung für Hochverfügbarkeit. Weitere Informationen finden Sie unter [Konfiguration von Mandanteneinstellungen](#).
- Ihre IaaS-Administratoren bereiten externe Ressourcen für die Bereitstellung vor. Weitere Informationen finden Sie unter [Externe Vorbereitungen für die Bereitstellung](#)
- Wenn Sie bei der Installation die Erstellung von anfänglichen Inhalten konfiguriert haben, kann der Konfigurationsadministrator das Katalogelement für anfängliche Inhalte anfordern, um ein Proof-of-Concept schnell aufzufüllen. Ein Beispiel zum Anfordern des Elements und zum Abschließen der manuellen Benutzeraktion finden Sie unter: [Szenario: Anfordern anfänglicher Inhalte für eine Rainpole-Proof-of-Concept-Bereitstellung](#).

Fehlerbehebung bei einer vRealize Automation -Installation

Die Fehlerbehebung bei vRealize Automation beschreibt Verfahren zur Lösung von Problemen, die bei der Installation oder Konfiguration von vRealize Automation auftreten können.

Standardspeicherorte für Protokolle

Informationen zu fehlgeschlagenen Installationen finden Sie in den System- und Produktprotokolldateien.

Hinweis Für die Protokollerfassung können Sie eventuell die vRealize Automation und vRealize Orchestrator Content Packs for vRealize Log Insight verwenden. Die Content Packs und Log Insight bieten eine konsolidierte Übersicht über Protokollereignisse für Komponenten der vRealize Suite. Weitere Informationen finden Sie auf der Website von [VMware Solution Exchange](#).

Die aktuelle Liste mit Protokollspeicherorten finden Sie im [VMware-Knowledgebase-Artikel 2141175](#).

Windows-Protokolle

Verwenden Sie folgenden Speicherort für die Suche nach Protokolldateien für Windows-Ereignisse.

Protokoll	Speicherort
Protokolle für Windows-Ereignisanzeige	Start > Systemsteuerung > Verwaltung > Ereignisanzeige

Installationsprotokolle

Installationsprotokolle befinden sich an den folgenden Speicherorten.

Protokoll	Standardspeicherort
Installationsprotokolle	C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log
WAPI-Installationsprotokolle	C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

IaaS-Protokolle

IaaS-Protokolle befinden sich an den folgenden Speicherorten.

Protokoll	Standardspeicherort
Website-Protokolle	C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs
Repository-Protokoll	C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Manager Service-Protokolle	C:\Program Files (x86)\VMware\vCAC\Server\Logs
DEM-Orchestrator-Protokolle	C:\Users\<Benutzername>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<Systemname> DEO \Logs
Agent-Protokolle	C:\Users\<Benutzername>\AppData\Local\Temp\VMware\vCAC\Agents\<Agent-Name>\logs

vRealize Automation Framework-Protokolle

Protokolleinträge für vRealize Automation-Frameworks befinden sich am folgenden Speicherort.

Protokoll	Standardspeicherort
Framework-Protokolle	/var/log/vmware

Protokolle für die Bereitstellung von Softwarekomponenten

Protokolle für die Bereitstellung von Softwarekomponenten befinden sich am folgenden Speicherort.

Protokoll	Standardspeicherort
Software-Agent-Bootstrap-Protokoll	/opt/vmware-appdirector (für Linux) oder \opt\vmware-appdirector (für Windows)
Protokolle für Softwarelebenszyklusskripts	/tmp/taskId (für Linux) \Users\darwin\AppData\Local\Temp\taskId (für Windows)

Protokollsammlung für verteilte Bereitstellungen

Sie können eine ZIP-Datei erstellen, in der alle Protokolle für Komponenten einer verteilten Bereitstellung gebündelt werden. .

Rollback einer fehlgeschlagenen Installation wird ausgeführt

Wenn eine Installation fehlschlägt und ein Rollback durchgeführt wird, muss der Systemadministrator sicherstellen, dass alle erforderlichen Dateien deinstalliert wurden, bevor eine weitere Installation gestartet wird. Einige Dateien müssen manuell deinstalliert werden.

Rollback einer Minimalinstallation ausführen

Ein Systemadministrator muss einige Dateien manuell entfernen und die Datenbank zurücksetzen, um eine fehlgeschlagene vRealize Automation-aaS-Installation vollständig installieren zu können.

Verfahren

- 1 Wenn die folgenden Komponenten vorhanden sind, deinstallieren Sie diese mit dem Windows-Deinstallationsprogramm.
 - vRealize Automation-Agents
 - vRealize Automation-DEM-Worker
 - vRealize Automation-DEM-Orchestrator
 - vRealize Automation-Server
 - vRealize Automation-WAPI

Hinweis Wenn die folgende Meldung angezeigt wird, starten Sie die Maschine neu und befolgen Sie die Schritte in diesem Verfahren: Fehler beim Öffnen der Installationsprotokolldatei. Stellen Sie sicher, dass der angegebene Speicherort vorhanden und nicht schreibgeschützt ist

Hinweis Wenn das Windows-System zurückgesetzt wurde oder SieaaS deinstalliert haben, müssen Sie den Befehl `iisreset` ausführen, bevor Sie vRealize Automation-aaS erneut installieren.

- 2 Setzen Sie Ihre Datenbank auf den Zustand zurück, der vor der Installation bestand. Die verwendete Methode hängt vom Installationsmodus der ursprünglichen Datenbank ab.
- 3 Wählen Sie in IIS (Internet Information Services) die Standard-Website (oder Ihre benutzerdefinierte Site) aus und klicken Sie auf **Bindungen**. Entfernen Sie die https-Bindung (standardmäßig 443).
- 4 Prüfen Sie, ob das Anwendungs-Repository, vRealize Automation und WAPI entfernt wurden, und ob die Anwendungspools RepositoryAppPool, vCACAppPool und WapiAppPool ebenso entfernt wurden.

Die Installation wurde vollständig entfernt.

Rollback einer verteilten Installation ausführen

Ein Systemadministrator muss einige Dateien manuell entfernen und die Datenbank zurücksetzen, um eine fehlgeschlagene IaaS-Installation vollständig installieren zu können.

Verfahren

- 1 Wenn die folgenden Komponenten vorhanden sind, deinstallieren Sie diese mit dem Windows-Deinstallationsprogramm.
 - vRealize Automation-Server
 - vRealize Automation-WAPI

Hinweis Wenn die folgende Meldung angezeigt wird, starten Sie die Maschine neu und führen Sie diesen Vorgang aus: Fehler beim Öffnen der Installationsprotokolldatei. Stellen Sie sicher, dass der angegebene Speicherort vorhanden und nicht schreibgeschützt ist.

Hinweis Wenn das Windows-System zurückgesetzt wurde oder Sie IaaS deinstalliert haben, müssen Sie den Befehl `iisreset` ausführen, bevor Sie vRealize Automation-IaaS erneut installieren.

- 2 Setzen Sie Ihre Datenbank auf den Zustand zurück, der vor der Installation bestand. Die verwendete Methode hängt vom Installationsmodus der ursprünglichen Datenbank ab.
- 3 Wählen Sie in IIS (Internet Information Services) die Standard-Website (oder Ihre benutzerdefinierte Site) aus und klicken Sie auf **Bindungen**. Entfernen Sie die https-Bindung (standardmäßig 443).
- 4 Prüfen Sie, ob das Anwendungs-Repository, vCAC und WAPI entfernt wurden, und ob die Anwendungspools RepositoryAppPool, vCACAppPool und WapiAppPool ebenso entfernt wurden.

Tabelle 1-44. Rollback-Fehlerpunkte

Fehlerpunkt	Aktion
Installieren von Manager Service	Sofern vorhanden, deinstallieren Sie vCloud Automation Center Server.
Installieren von DEM-Orchestrator	Deinstallieren Sie den DEM-Orchestrator, sofern vorhanden.
Installieren von DEM Worker	Deinstallieren Sie alle DEM-Worker, sofern vorhanden.
Installieren eines Agents	Deinstallieren Sie alle vRealize Automation-Agents, sofern vorhanden.

Erstellen eines vRealize Automation -Support-Pakets

Sie können ein vRealize Automation-Support-Paket unter Verwendung der Verwaltungsschnittstelle der vRealize Automation-Appliance erstellen. Support-Pakete erfassen Protokolle und helfen Ihnen oder dem technischen Support von VMware bei der Behebung von vRealize Automation-Problemen.

Verfahren

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

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

- 2 Melden Sie sich als Root-Benutzer an und klicken Sie auf **vRA-Einstellungen > Cluster**.

- 3 Klicken Sie auf **Support-Paket erstellen**.

- 4 Klicken Sie auf **Herunterladen** und speichern Sie die Support-Paket-Datei auf Ihrem System.

Support-Pakete enthalten Informationen aus der vRealize Automation-Appliance und den IaaS-Windows-Servern. Wenn die Verbindung zwischen der vRealize Automation-Appliance und den IaaS-Komponenten unterbrochen wird, fehlen im Support-Paket möglicherweise die Protokolle der IaaS-Komponente.

Wenn Sie wissen möchten, welche Protokolldateien erfasst wurden, entpacken Sie das Support-Paket und öffnen Sie die Datei `Environment.html` in einem Webbrowser. Wenn keine Verbindung besteht, werden die IaaS-Komponenten in der Tabelle „Knoten“ möglicherweise in Rot angezeigt. Ein weiterer Grund für das Fehlen der IaaS-Protokolle könnte darin liegen, dass der Management-Agent-Dienst von vRealize Automation auf IaaS-Windows-Servern, die in Rot angezeigt werden, angehalten wurde.

Allgemeine Fehlerbehebung bei der Installation

Die Themen zur Fehlerbehebung für vRealize Automation-Appliances liefern Lösungen für potenzielle Probleme im Zusammenhang mit der Installation, die bei der Verwendung von vRealize Automation auftreten können.

Installations- oder Aktualisierungsfehler mit einem Zeitüberschreitungsfehler des Lastausgleichsdiensts

Ein(e) vRealize Automation-Installation bzw. -Upgrade für eine verteilte Bereitstellung mit einem Lastausgleichsdienst schlägt mit Fehler 503 „Dienst nicht verfügbar“ fehl.

Problem

Die Installation bzw. das Upgrade schlägt fehl, da der Zeitüberschreitungswert für den Lastausgleichsdienst nicht genügend Zeit zum Abschluss der Aufgabe einräumt.

Ursache

Ein unzureichender Zeitüberschreitungswert für den Lastausgleichsdienst kann zu einem Fehler führen. Sie können das Problem beheben, indem Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden erhöhen und die Aufgabe erneut ausführen.

Lösung

- 1 Erhöhen Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden.
- 2 Führen Sie die Installation bzw. das Upgrade erneut aus.

Serverzeiten sind nicht synchronisiert

Eine Installation ist möglicherweise nicht erfolgreich, wenn die IaaS-Zeitserver nicht mit der vRealize Automation-Appliance synchronisiert sind.

Problem

Sie können sich nach der Installation nicht anmelden, da ansonsten die Installation während der Fertigstellung fehlschlägt.

Ursache

Die Zeitserver auf allen Servern sind möglicherweise nicht synchronisiert.

Lösung

Synchronisieren Sie alle vRealize Automation-Appliances und IaaS-Windows-Server auf die gleiche Zeitquelle. Verwenden Sie innerhalb einer vRealize Automation-Bereitstellung niemals verschiedene Zeitquellen.

- Legen Sie eine vRealize Automation-Appliance Zeitquelle fest:
 - a Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.

`https://vrealize-automation-appliance-FQDN:5480`
 - b Wählen Sie **Admin > Uhrzeiteinstellungen** aus und legen Sie die Quelle für die Uhrzeitsynchronisierung fest.

Option	Beschreibung
Hostuhrzeit	Mit ESXi-Host der vRealize Automation-Appliance synchronisieren.
Zeitserver	Mit externem Network Time Protocol (NTP)-Server synchronisieren. Geben Sie den FQDN oder die IP-Adresse des NTP-Servers ein.

- Informationen zu IaaS-Windows-Servern finden Sie unter [Aktivieren der Zeitsynchronisierung auf dem Windows-Server](#).

Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 werden möglicherweise leere Seiten angezeigt

Wenn Sie Internet Explorer 9 oder 10 unter Windows 7 verwenden und der Kompatibilitätsmodus aktiviert ist, scheinen manche Seiten keinen Inhalt aufzuweisen.

Problem

Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 weisen die folgenden Seiten keinen Inhalt auf:

- Infrastruktur
- Standardmandantenordner auf der Orchestrator-Seite
- Serverkonfiguration auf der Orchestrator-Seite

Ursache

Dieses Problem könnte darauf zurückzuführen sein, dass der Kompatibilitätsmodus aktiviert ist. Den Kompatibilitätsmodus können Sie für Internet Explorer wie folgt deaktivieren.

Lösung

Voraussetzungen

Stellen Sie sicher, dass die Menüleiste angezeigt wird. Wenn Sie Internet Explorer 9 oder 10 verwenden, drücken Sie die Alt-Taste, um die Menüleiste anzuzeigen (oder klicken Sie mit der rechten Maustaste auf die Adressleiste und wählen Sie **Menüleiste** aus).

Verfahren

- 1 Wählen Sie **Extras > Einstellungen der Kompatibilitätsansicht** aus.
- 2 Deaktivieren Sie **Intranetsites in Kompatibilitätsansicht anzeigen**.
- 3 Klicken Sie auf **Schließen**.

Es kann kein Vertrauensverhältnis für den sicheren SSL/TLS-Kanal hergestellt werden

Beim Upgrade von Sicherheitszertifikaten für vCloud Automation Center wird möglicherweise die Fehlermeldung „Es kann kein Vertrauensverhältnis für den sicheren SSL/TLS-Kanal hergestellt werden“ angezeigt.

Problem

Wenn ein Zertifikatfehler mit „vcac-config.exe“ beim Upgrade eines Sicherheitszertifikats auftritt, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
Die zugrunde liegende Verbindung wurde getrennt: Es konnte kein Vertrauensverhältnis für den sicheren SSL/TLS-Kanal hergestellt werden
```

Weitere Informationen zur Ursache dieses Problems erhalten Sie wie nachfolgend beschrieben.

Lösung

- 1 Öffnen Sie im Texteditor `vcac-config.exe.config` und suchen Sie die Repository-Adresse:
`<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />`
- 2 Öffnen Sie die Adresse im Internet Explorer.
- 3 Klicken Sie in angezeigten Fehlermeldungen wegen der Zertifikatvertrauensstellung auf „Weiter“.

- 4 Rufen Sie in Internet Explorer einen Sicherheitsbericht ab und stellen Sie damit fest, weshalb das Zertifikat nicht vertrauenswürdig ist.

Falls die Probleme weiterhin bestehen, wiederholen Sie den Vorgang mit der Adresse, die registriert werden muss, nämlich der Endpoint-Adresse, die Sie zum Registrieren mit `vcac-config.exe` verwendet haben.

Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server

Bestimmte Sites stellen unter Umständen über einen Proxy-Server eine Verbindung zum Internet her.

Problem

Ihre Bereitstellung kann keine Verbindung zum offenen Internet herstellen. Sie können beispielsweise nicht auf Websites, öffentliche Clouds, die von Ihnen verwaltet werden, oder Anbieteradressen zugreifen, die Sie zum Herunterladen von Software oder Updates benötigen.

Ursache

Ihre Site stellt über einen Proxy-Server eine Verbindung zum Internet her.

Lösung

Voraussetzungen

Bitten Sie den Administrator der Site, Ihnen Proxy-Servernamen, Portnummern und Anmeldedaten bereitzustellen.

Verfahren

- 1 Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Melden Sie sich als Root-Benutzer an und klicken Sie auf **Netzwerk**.
- 3 Geben Sie den FQDN oder die IP-Adresse und Portnummer des Proxy-Servers Ihrer Site ein.
- 4 Benötigt der Proxy-Server Anmeldedaten, geben Sie den Benutzernamen und das Kennwort ein.
- 5 Klicken Sie auf **Einstellungen speichern**.

Nächste Schritte

Die Konfiguration zur Verwendung eines Proxy-Servers wirkt sich unter Umständen auf den VMware Identity Manager-Benutzerzugriff aus. Informationen zur Behebung dieses Problems finden Sie unter [Proxy verhindert VMware Identity Manager-Benutzeranmeldung](#).

Konsolenschritte für die Erstkonfiguration von Inhalten

Es steht eine Alternative zur Verwendung der vRealize Automation-Installationsschnittstelle zum Erstellen des Kontos für den Konfigurationsadministrator und des anfänglichen Inhalts zur Verfügung.

Problem

Im letzten Teil der Installation von vRealize Automation führen Sie das Verfahren zum Erstellen eines neuen Kontos, des lokalen Benutzerkontos „configurationadmin“ und des anfänglichen Inhalts durch. Ein Fehler tritt auf und die Schnittstelle wird in einen nicht behebbaren Zustand versetzt.

Lösung

Statt die Schnittstelle zu verwenden, geben Sie Konsolenbefehle ein, um den Benutzer „configurationadmin“ und den anfänglichen Inhalt zu erstellen. Beachten Sie, dass die Schnittstelle möglicherweise erst nach der erfolgreichen Durchführung eines Teils des Verfahrens ausfällt, sodass Sie ggf. nur einige der Befehle benötigen.

Angenommen, Sie untersuchen die Protokolle und die Ausführung des vRealize Orchestrator-Workflows und stellen dabei fest, dass der Benutzer „configurationadmin“ durch das schnittstellenbasierte Setup erstellt wurde, der anfängliche Inhalt aber nicht. In diesem Fall können Sie einfach die letzten beiden Konsolenbefehle eingeben, um das Verfahren abzuschließen.

Verfahren

- 1 Melden Sie sich bei der Konsole der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Importieren Sie den vRealize Orchestrator-Workflow durch Eingabe des folgenden Befehls:

```
/usr/sbin/vcac-config -e content-import --workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 Führen Sie den Workflow aus, um den Benutzer „configurationadmin“ zu erstellen:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflow-executor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 Importieren Sie den ASD-Blueprint durch Eingabe des folgenden Befehls:

```
/usr/sbin/vcac-config -e content-import --blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 Führen Sie den Workflow aus, um den anfänglichen Inhalt zu konfigurieren:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflow-executor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

vRealize Automation -Lizenzen können nicht herabgestuft werden

Ein Fehler tritt auf, wenn Sie den Lizenzschlüssel einer niedrigeren Produktedition senden.

Problem

Die folgende Meldung wird angezeigt, wenn die Seite für die Lizenzierung der Verwaltungsschnittstelle von vRealize Automation verwendet wird, um den Lizenzschlüssel an eine Produktedition zu senden, die niedriger als die aktuelle ist. Sie beginnen beispielsweise mit einer Enterprise-Lizenz und versuchen, eine erweiterte Lizenz einzugeben.

```
Unable to downgrade existing license edition
```

Ursache

Diese Version von vRealize Automation unterstützt nicht die Herabstufung von Lizenzen. Sie können nur Lizenzen einer gleichen oder höheren Edition hinzufügen.

Lösung

Um auf eine niedrigere Edition zu wechseln, installieren Sie vRealize Automation erneut.

Fehlerbehebung bei der vRealize Automation -Appliance

Die Fehlerbehebungsthemen für vRealize Automation-Appliances bieten Lösungen für mögliche Probleme im Zusammenhang mit der Installation, auf die Sie stoßen können, wenn Sie Ihre vRealize Automation-Appliances verwenden.

Installationsprogramme können nicht heruntergeladen werden

Installationsprogramme können nicht von der vRealize Automation-Appliance heruntergeladen werden.

Problem

Die Installationsprogramme werden nicht heruntergeladen, wenn `setup__vrealize-automation-appliance-FQDN@5480.exe` ausgeführt wird.

Ursache

- Probleme mit der Netzwerkkonnektivität beim Herstellen der Verbindung zur vRealize Automation-Appliance.
- Herstellung der Verbindung zur vRealize Automation-Appliance ist nicht möglich, da die Maschine nicht erreichbar ist oder nicht reagieren kann, bevor die Zeitbegrenzung der Verbindung überschritten wird.

Lösung

- 1 Stellen Sie sicher, dass Sie eine Verbindung zur vRealize Automation-URL in einem Webbrowser herstellen können.
`https://vrealize-automation-appliance-FQDN`
- 2 Lesen Sie die anderen Abschnitte zur Fehlerbehebung für die vRealize Automation-Appliance.
- 3 Laden Sie die Setupdatei herunter und stellen Sie die Verbindung zur vRealize Automation-Appliance erneut her.

Falsche Berechtigungen für die Datei „Encryption.key“

Ein Systemfehler kann verursacht werden, wenn der Datei „Encryption.key“ für eine virtuelle Appliance falsche Berechtigungen zugewiesen werden.

Problem

Sie melden sich bei der vRealize Automation-Appliance an und die Seite „Mandanten“ wird angezeigt. Nachdem das Laden der Seite gestartet wurde, wird die Meldung Systemfehler angezeigt.

Ursache

Die Datei „Encryption.key“ weist falsche Berechtigungen auf oder die Gruppen- oder Besitzerbenutzer-ebene ist nicht ordnungsgemäß zugewiesen.

Lösung

Voraussetzungen

Melden Sie sich bei der virtuellen Appliance an, in der die Fehlermeldung angezeigt wird.

Hinweis Wenn Ihre virtuellen Appliances unter einem Lastausgleichsdienst ausgeführt werden, müssen Sie jede virtuelle Appliance überprüfen.

Verfahren

- 1 Zeigen Sie die Protokolldatei `/var/log/vcac/catalina.out` an und suchen Sie nach der Meldung `Cannot write to /etc/vcac/Encryption.key`.
- 2 Wechseln Sie zum Verzeichnis `/etc/vcac/` und überprüfen Sie die Berechtigungen und Besitzrechte für die Datei „Encryption.key“. Eine Zeile ähnlich der Folgenden sollte angezeigt werden:

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Lese- und Schreibberechtigungen sind erforderlich und der Besitzer und die Gruppe für die Datei muss `vcac` sein.

- 3 Wenn die Ausgabe davon abweicht, ändern Sie ggf. die Berechtigungen oder Besitzrechte der Datei.

Nächste Schritte

Melden Sie sich bei der Seite „Mandanten“ an, um sicherzustellen, dass Sie sich problemlos anmelden können.

Identity Manager der Verzeichnisverwaltung startet nach einem Neustart von horizon-workspace nicht

In einer vRealize Automation-Umgebung mit Hochverfügbarkeit kann es vorkommen, dass der Identity Manager der Verzeichnisverwaltung nach einem Neustart des horizon-workspace-Diensts nicht startet.

Problem

Der horizon-workspace-Dienst kann aufgrund eines Fehlers wie dem Folgenden nicht starten:

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Ursache

Der Identity Manager startet möglicherweise in einer Hochverfügbarkeitsumgebung aufgrund von Problemen mit dem liquibase-Datenverwaltungsdienstprogramm nicht, das von vRealize Automation verwendet wird.

Lösung

1 Melden Sie sich als Root-Benutzer bei einer Konsolensitzung auf der vRealize Automation-Appliance an.

2 Beenden Sie den horizon-workspace-Dienst durch Eingabe des folgenden Befehls.

```
#service horizon-workspace stop
```

3 Öffnen Sie die Postgres-Shell als Superuser.

```
su postgres
```

4 Navigieren Sie zum richtigen Bin-Verzeichnis.

```
cd /opt/vmware/vpostgres/current/bin
```

5 Stellen Sie eine Verbindung zur Datenbank her.

```
psql vcac
```

6 Führen Sie von `saas.databasechangelock` aus die folgende SQL-Abfrage aus.

```
select * from databasechangelock;
```

Wenn die Ausgabe den Wert „t“ für „true“ anzeigt, muss die Sperre manuell aufgehoben werden.

7 Wenn Sie die Sperre manuell aufheben müssen, führen Sie die folgende SQL-Abfrage aus.

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL, locke-
dby=NULL where id=1;
```

8 Führen Sie von `saas.databasechangelock` aus die folgende SQL-Abfrage aus.

```
select * from databasechangelock;
```

Die Ausgabe sollte den Wert „f“ für „false“ anzeigen. Dies bedeutet, dass die Sperre aufgehoben ist.

9 Beenden Sie die Postgres-VCAC-Datenbank.

```
vcac=# \q
```

10 Schließen Sie die Postgres-Shell.

```
exit
```

11 Starten Sie den horizon-workspace-Dienst.

```
#service horizon-workspace start
```

Falsche Zuweisungen von Appliance-Rollen nach Failover

Nachdem ein Failover stattgefunden hat, haben die Master- und Replikatknoten der vRealize Automation-Appliance möglicherweise nicht die richtige Rollenzuweisung. Davon sind alle Dienste betroffen, die Schreibzugriff für die Datenbank benötigen.

Problem

In einem Hochverfügbarkeitscluster mit vRealize Automation-Appliances fahren Sie den Master-Datenbankknoten herunter oder sorgen dafür, dass kein Zugriff darauf mehr möglich ist. Über die Verwaltungskonsole auf einem anderen Knoten stufen Sie diesen Knoten zum neuen Master-Knoten herauf. Dadurch wird der Schreibzugriff auf die vRealize Automation-Datenbank wiederhergestellt.

Zu einem späteren Zeitpunkt stellen Sie den alten Master-Knoten wieder online. Auf der Registerkarte „Datenbank“ in der Verwaltungskonsole dieses Knotens wird dieser weiterhin als Master-Knoten aufgeführt, obwohl er es nicht ist. Versuche, das Problem über die Verwaltungskonsole eines anderen Knotens zu lösen, indem der alte Knoten offiziell wieder zum Master-Knoten heraufgestuft wird, schlagen fehl.

Lösung

Befolgen Sie bei einem Failover diese Richtlinien beim Konfigurieren von alten im Vergleich zu neuen Master-Knoten.

- Bevor Sie einen anderen Knoten zum Master-Knoten heraufstufen, entfernen Sie den vorherigen Master-Knoten aus dem Lastenausgleichspool von vRealize Automation-Appliance-Knoten.
- Damit vRealize Automation einen alten Master-Knoten wieder in den Cluster übernimmt, muss die alte Maschine online geschaltet werden. Öffnen Sie anschließend die Verwaltungskonsole des neuen Master-Knotens. Suchen Sie nach dem alten Knoten, der auf der Registerkarte „Datenbank“ als `invalid` aufgeführt ist, und klicken Sie auf die Schaltfläche **Zurücksetzen**.

Nach dem erfolgreichen Zurücksetzen können Sie den alten Knoten im Lastenausgleichspool der vRealize Automation-Appliance-Knoten wiederherstellen.

- Um einen alten Master-Knoten manuell wieder in den Cluster zu übernehmen, schalten Sie die Maschine online und fügen Sie sie dem Cluster so hinzu, als handelte es sich um einen neuen Knoten. Geben Sie beim Hinzufügen den neu heraufgestuften Knoten als primären Knoten an.

Nachdem der Knoten erfolgreich hinzugefügt wurde, können Sie den alten Knoten im Lastenausgleichspool der vRealize Automation-Appliance-Knoten wiederherstellen.

- Verwenden Sie die Verwaltungskonsole eines alten Master-Knotens erst wieder für Clusterverwaltungsvorgänge, nachdem der alte Master-Knoten ordnungsgemäß zurückgesetzt oder dem Cluster wieder hinzugefügt wurde, auch wenn der Knoten wieder online geschaltet wurde.

- Nachdem Sie den Knoten ordnungsgemäß zurückgesetzt oder wieder hinzugefügt haben, können Sie einen alten Knoten wieder zum Master-Knoten heraufstufen.

Fehler nach dem Upgrade von Replikat- und Master-Knoten

Ein Problem mit dem Festplattenspeicher gemeinsam mit der Hochstufung von Replikat- und Master-Datenbankknoten der vRealize Automation-Appliance kann zu Bereitstellungsproblemen führen.

Problem

Der Master-Knoten hat keinen Festplattenspeicher mehr. Sie melden sich bei der Verwaltungsschnittstelle der Datenbank an und stufen einen Replikat-Knoten zum neuen Master-Knoten hoch. Die Hochstufung ist erfolgreich, wenn Sie die Verwaltungsschnittstellenseite aktualisieren können, auch wenn eine Fehlermeldung aufgetreten ist.

In einem weiteren Schritt geben Sie Festplattenspeicher auf dem alten Knoten frei. Nach der Hochstufung des Knotens zum Master schlägt die Bereitstellung fehl und bleibt bei IN_PROGRESS hängen.

Ursache

vRealize Automation kann die alte Master-Knotenkonfiguration nicht richtig aktualisieren, wenn nicht ausreichend Speicherplatz vorhanden ist.

Lösung

Wenn die Verwaltungsschnittstelle während der Hochstufung Fehler zeigt, schließen Sie den Knoten vorübergehend aus dem Lastausgleichsdienst aus. Korrigieren Sie das Knotenproblem, indem Sie beispielsweise Festplattenspeicher hinzufügen, bevor Sie den Lastausgleichsdienst wieder hinzufügen. Aktualisieren Sie dann die Verwaltungsschnittstellenseite der Datenbank und überprüfen Sie, ob die richtigen Master- und Replikat-Knoten vorhanden sind.

Falsche vRealize Automation Komponentendienstregistrierungen

Die Verwaltungsschnittstelle der vRealize Automation-Appliance kann bei der Lösung von Registrierungsproblemen bei vRealize Automation-Komponentendiensten hilfreich sein.

Problem

Unter normalen Umständen müssen alle vRealize Automation-Komponentendienste eindeutig und REGISTRIERT sein. Alle anderen Bedingungen könnten zu unvorhersehbarem Verhalten von vRealize Automation führen.

Ursache

Im Folgenden sehen Sie Beispiele von Problemen, die mit den vRealize Automation-Komponentendiensten auftreten können.

- Ein Dienst ist inaktiv geworden.
- Die Servereinstellungen haben dazu geführt, dass ein Dienst nicht mehr als REGISTRIERT eingetragen ist.

- Eine Abhängigkeit von einem anderen Dienst hat dazu geführt, dass ein Dienst nicht mehr als REGISTRIERT eingetragen ist.

Lösung

Registrieren Sie Komponentendienste erneut, die offenbar Probleme aufweisen.

- 1 Erstellen Sie einen Snapshot der vRealize Automation-Appliance.

Möglicherweise müssen Sie den Dienst auf den Snapshot zurücksetzen, wenn Sie verschiedene Dienständerungen ausprobieren und sich die Appliance schließlich in einem unvorhersehbaren Zustand befindet.

- 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 **Dienste**.

- 4 Suchen Sie in der Liste der Dienste einen Dienst, der sich nicht im richtigen Zustand befindet oder andere Probleme aufweist.

- 5 Wenn ein fehlerhafter Dienst `iaas-service` ist, fahren Sie mit dem nächsten Schritt fort.

Melden Sie sich andernfalls zur erneuten Registrierung des vRealize Automation-Dienstes bei einer Konsolensitzung in der vRealize Automation-Appliance als Root-Benutzer an und starten Sie vRealize Automation neu, indem Sie folgenden Befehl eingeben.

```
service vcac-server restart
```

Bei Diensten, die mit der eingebetteten vRealize Orchestrator-Instanz verbunden sind, geben Sie folgenden zusätzlichen Befehl ein.

```
service vco-restart restart
```

- 6 Wenn es sich bei einem fehlerhaften Dienst um `iaas-service` handelt, führen Sie die folgenden Schritte aus, um den Dienst erneut zu registrieren.

- a Heben Sie die Registrierung des Diensts nicht auf.
- b Melden Sie sich auf dem primären IaaS-Webserver mit einem Konto mit Administratorrechten an.
- c Öffnen Sie als Administrator eine Eingabeaufforderung.
- d Führen Sie folgenden Befehl aus.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url https://Appliance-oder-Lastausgleichs-dienst-IP-oder-FQDN/ -t vsphere.local -cu administrator -cp Kennwort -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Das Kennwort ist das Kennwort von `administrator@vsphere.local`.

- e Führen Sie einen Befehl zum Aktualisieren der Registrierungsinformationen in der IaaS-Datenbank aus.

SQL Server mit Windows-Authentifizierung:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s IaaS-SQL-Server-IP-oder-FQDN -d SQL-Datenbankname -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

SQL Server mit nativer SQL-Authentifizierung:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s SQL-Server-IP-oder-FQDN -d SQL-Datenbankname -su SQL-Benutzer -sp SQL-Benutzerkennwort -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Den Server- oder Datenbanknamen finden Sie, indem Sie die folgende Datei in einem Texteditor öffnen und nach repository suchen. Die Werte für die Datenquelle und den anfänglichen Katalog geben jeweils Aufschluss über die Serveradresse und den Datenbanknamen.

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

Der SQL-Benutzer muss über DBO-Berechtigungen auf der Datenbank verfügen.

- f Registrieren Sie die Endpoints, indem Sie die folgenden Befehle ausführen:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Webserver-oder-Lastausgleichsdienst-IP-oder-FQDN /vcac --Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Webserver-oder-Lastausgleichsdienst-IP-oder-FQDN /WAPI --Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Webserver-oder-Lastausgleichsdienst-IP-oder-FQDN /repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Webserver-oder-Lastausgleichsdienst-IP-oder-FQDN /WAPI/api/status --Endpoint status -v
```

- g Registrieren Sie Katalogelemente, indem Sie den folgenden Befehl ausführen:

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

- h Starten Sie IIS neu.

```
iisreset
```

- i Melden Sie sich beim primären IaaS Manager Service-Host an.

- j Starten Sie den vRealize Automation-Windows-Dienst neu.

```
VMware vCloud Automation Center Service
```

- Um Dienste in Verbindung mit einem externen System wie zum Beispiel eine externe vRealize Orchestrator-Instanz erneut zu registrieren, melden Sie sich bei dem externen System an und starten Sie den Dienst dort neu.

Zusätzliche Netzwerkkarte (NIC) verursacht Fehler bei der Verwaltungsschnittstelle

Nachdem Sie einer vRealize Automation-Appliance eine zweite Netzwerkkarte (NIC) hinzugefügt haben, werden einige Seiten der vRealize Automation-Verwaltungsschnittstelle nicht ordnungsgemäß geladen.

Problem

Sie haben eine zweite Netzwerkkarte erfolgreich über vCenter hinzugefügt, und die folgenden Seiten der vRealize Automation-Verwaltungsschnittstelle werden nicht geladen. Stattdessen werden Fehler angezeigt.

- Die Seite **Netzwerk > Status** zeigt eine Fehlermeldung an, die sich auf ein nicht antwortendes Skript bezieht.
- Die Seite **Netzwerk > Adresse** zeigt eine Fehlermeldung an, die sich darauf bezieht, dass Netzwerkkarteninformationen nicht gelesen werden konnten.

Ursache

Ab Version 7.3 unterstützt die vRealize Automation-Appliance zwei Netzwerkkarten (NICs). Die Engineering-Vorlage, auf der die Appliance basiert, verhindert jedoch eine ordnungsgemäße Funktion der Verwaltungsschnittstelle, bis Sie die Lösung anwenden.

Lösung

Starten Sie die vRealize Automation-Appliance neu, nachdem Sie eine zusätzliche Netzwerkkarte (NIC) hinzugefügt haben.

Heraufstufen einer sekundären virtuellen Appliance zum Master ist nicht möglich

In vRealize Automation verhindert geringer Arbeitsspeicher einer virtuellen Appliance möglicherweise, dass sie im Cluster heraufgestuft wird.

Problem

Der Masterknoten verfügt über wenig Arbeitsspeicher. Sie melden sich bei der Datenbankseite der Verwaltungsschnittstelle an und stufen einen sekundären Knoten zum neuen Masterknoten hoch. Der folgende Fehler tritt auf:

```
Fail to execute on Node Knotenname, host is Master-FQDN
because of: Could not read remote lock command result for node: Knotenname
on address: Master-FQDN, reason is: 500 Internal Server Error
```

Ursache

Das Heraufstufen ist nur dann erfolgreich, wenn alle Knoten die Neukonfiguration zu einem neu heraufgestuften Masterknoten bestätigen können. Der geringe Arbeitsspeicher verhindert die Bestätigung durch den alten Masterknoten, auch wenn alle Knoten erreichbar sind.

Lösung

Schalten Sie den Masterknoten mit dem geringen Arbeitsspeicher aus. Melden Sie sich bei der Datenbankseite der Verwaltungsschnittstelle des sekundären Knotens an und stufen Sie den sekundären Knoten herauf.

Der Aufbewahrungszeitraum des Active Directory-Synchronisierungsprotokolls ist zu kurz

In vRealize Automation reichen die Active Directory-Synchronisierungsprotokolle nur zwei Tage in die Vergangenheit.

Problem

Nach zwei Tagen werden Active Directory-Synchronisierungsprotokolle in der Verwaltungsschnittstelle nicht mehr angezeigt. Auch die Ordner für die Protokolle werden im folgenden Verzeichnis der vRealize Automation-Appliance nicht mehr angezeigt:

```
/db/elasticsearch/horizon/nodes/0/indices
```

Ursache

Um Speicherplatz einzusparen, setzt vRealize Automation den maximalen Aufbewahrungszeitraum für Active Directory-Synchronisierungsprotokolle auf drei Tage.

Lösung

- 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.
`/usr/local/horizon/conf/runtime-config.properties`
- 3 Erhöhen Sie den Wert der Eigenschaft `analytics.maxQueryDays`.
- 4 Speichern und schließen Sie `runtime-config.properties`.
- 5 Starten Sie den Identity Manager und die elastischen Suchdienste neu.

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ kann Hostnamen nicht auflösen

RabbitMQ verwendet standardmäßig kurze Hostnamen für vRealize Automation-Appliances, was die gegenseitige Auflösung von Knoten verhindern kann.

Problem

Sie versuchen, eine andere vRealize Automation-Appliance zum Cluster hinzuzufügen, und ein Fehler ähnlich dem folgenden tritt auf.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for details.
```

Ursache

Ihre Netzwerkkonfiguration lässt nicht zu, dass vRealize Automation-Appliances sich gegenseitig anhand von kurzen Hostnamen auflösen.

Lösung

- 1 Melden Sie sich für alle vRealize Automation-Appliances in der Bereitstellung in einer Konsolensitzung als Root-Benutzer an.
- 2 Halten Sie den RabbitMQ-Dienst an.
`service rabbitmq-server stop`
- 3 Öffnen Sie die folgende Datei in einem Texteditor.
`/etc/rabbitmq/rabbitmq-env.conf`
- 4 Legen Sie für die folgende Eigenschaft den Wert „true“ fest.
`USE_LONGNAME=true`
- 5 Speichern und schließen Sie `rabbitmq-env.conf`.
- 6 Setzen Sie RabbitMQ zurück.
`vcac-vami rabbitmq-cluster-config reset-rabbitmq-node`
- 7 Führen Sie das folgende Skript auf nur einem vRealize Automation-Appliance-Knoten aus.
`vcac-config cluster-config-ping-nodes --services rabbitmq-server`

- 8 Stellen Sie auf allen Knoten sicher, dass der RabbitMQ-Dienst gestartet wurde.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

Fehlerbehebung bei IaaS-Komponenten

Die Themen zur Fehlerbehebung für vRealize Automation-IaaS-Komponenten liefern Lösungen für potenzielle Probleme im Zusammenhang mit der Installation, die bei der Verwendung von vRealize Automation auftreten können.

Voraussetzungskorrektur kann keine .NET-Funktionen installieren

Die Option **Korrigieren** der vRealize Automation-Voraussetzungskorrektur schlägt fehl und zeigt Meldungen an, die besagen, dass die Installationsquelle für .NET 3.5.1 nicht gefunden wurde.

Problem

Die Voraussetzungsprüfung muss sicherstellen, dass .NET 3.5.1 installiert ist, um die Anforderungen für Windows Server 2008 R2-Systeme mit IIS 7.5 und Windows Server 2012 R2-Systeme mit IIS 8 zu erfüllen.

Ursache

Bei Windows Server 2012 R2 kann die automatische Installation von .NET verhindert werden, wenn keine Installation mit dem Internet hergestellt werden kann. Bestimmte Windows 2012 R2-Updates können die Installation ebenfalls verhindern. Das Problem tritt auf, weil die Windows-Version nicht über eine lokale Kopie der .NET Framework 3.5-Installationsquelle verfügt.

Lösung

Geben Sie manuell eine .NET Framework 3.5-Installationsquelle an.

- 1 Mounten Sie auf dem Windows-Host ein ISO-Image der Windows Server 2012 R2-Installationsmedien.
- 2 Aktivieren Sie im Server Manager .NET Framework 3.5 mithilfe des Assistenten zum Hinzufügen von Rollen und Funktionen.
- 3 Navigieren Sie während der Ausführung des Assistenten zum .NET Framework 3.5-Installationspfad auf den ISO-Medien.
- 4 Nachdem Sie .NET Framework 3.5 hinzugefügt haben, führen Sie die vRealize Automation-Voraussetzungsprüfung erneut aus.

Überprüfen der Server-Zertifikate für IaaS

Sie können den Befehl `vcac-Config.exe` verwenden, um sicherzustellen, dass ein IaaS-Server vRealize Automation-Appliance- und SSO-Appliance-Zertifikate akzeptiert.

Problem

Wenn Sie IaaS-Funktionen verwenden, werden Autorisierungsfehler angezeigt.

Ursache

Autorisierungsfehler können auftreten, wenn IaaS die Sicherheitszertifikate von anderen Komponenten nicht erkennt.

Lösung

- 1 Öffnen Sie als Administrator eine Eingabeaufforderung und navigieren Sie zum Cafe-Verzeichnis unter `vra-installation-dir\Server\Model Manager Data\Cafe`, in der Regel `C:\Programme (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Geben Sie einen Befehls im Format `Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v` ein. Optionale Parameter sind `-su [SQL user name]` und `-sp [password]`.

Ist der Befehl erfolgreich, wird die folgende Meldung angezeigt:

```
Certificates validated successfully.  
Command succeeded.
```

Schlägt der Befehl fehl, wird eine detaillierte Fehlermeldung angezeigt.

Hinweis Dieser Befehl ist nur auf dem Knoten für die Model Manager-Datenkomponente verfügbar.

Fehler aufgrund der Anmeldedaten beim Ausführen des IaaS-Installers

Wenn Sie IaaS-Komponenten installieren, erhalten Sie eine Fehlermeldung bei der Eingabe der Anmeldedaten für die virtuelle Appliance.

Problem

Nach der Eingabe der Anmeldedaten in den IaaS-Installer wird ein `org.xml.sax.SAXParseException`-Fehler angezeigt.

Ursache

Sie haben falsche Anmeldedaten oder ein falsches Format für die Anmeldedaten verwendet.

Lösung

- ◆ Stellen Sie sicher, dass Sie die richtigen Mandanten- und Benutzernamenwerte verwenden.

Der SSO-Standardmandant verwendet beispielsweise einen Domännennamen wie `vsphere.local`, jedoch nicht `administrator@vsphere.local`.

Warnung wegen Speicherung der Einstellungen wird während IaaS-Installation angezeigt

Eine Meldung ähnlich der Folgenden wird während der IaaS-Installation angezeigt: Warnung: Die Einstellungen konnten während der IaaS-Installation nicht in der virtuellen Appliance gespeichert werden.

Problem

Während der IaaS-Installation wird fälschlicherweise eine Fehlermeldung angezeigt, dass die Benutzereinstellungen nicht gespeichert wurden.

Ursache

Dies kann auf Kommunikations- oder Netzwerkprobleme zurückzuführen sein.

Lösung

Ignorieren Sie die Fehlermeldung und fahren Sie mit der Installation fort. Die Installation sollte aufgrund dieser Fehlermeldung nicht fehlschlagen.

Fehler beim Installieren des Website-Servers und der Distributed Execution Manager

Die Installation des Website-Servers und der Distributed Execution Manager der Infrastruktur der vRealize Automation-Appliance kann nicht fortgesetzt werden, wenn das Kennwort für Ihr IaaS-Dienstkonto doppelte Anführungszeichen enthält.

Problem

Es wird eine Nachricht angezeigt, mit der Sie informiert werden, dass die Installation der Distributed Execution Manager (DEMs) und Website-Server der vRealize Automation-Appliance aufgrund ungültiger msixexec-Parameter fehlgeschlagen ist.

Ursache

Beim Kennwort für das IaaS-Dienstkonto wird ein doppeltes Anführungszeichen verwendet.

Lösung

- 1 Stellen Sie sicher, dass im Kennwort für Ihr IaaS-Dienstkonto keine doppelten Anführungszeichen enthalten sind.
- 2 Wenn Ihr Kennwort doppelte Anführungszeichen enthält, erstellen Sie ein neues Kennwort.
- 3 Starten Sie die Installation neu.

IaaS-Authentifizierung schlägt während der Installation der IaaS-Web- und Modellverwaltung fehl

Bei der Ausführung der Voraussetzungsprüfung wird eine Meldung angezeigt, dass die IIS-Authentifizierungsprüfung fehlgeschlagen ist.

Problem

Diese Fehlermeldung besagt, dass die Authentifizierung nicht aktiviert ist, aber das Kontrollkästchen für die IIS-Authentifizierung ist aktiviert.

Lösung

- 1 Deaktivieren Sie das Kontrollkästchen „Windows-Authentifizierung“.
- 2 Klicken Sie auf **Speichern**.

- 3 Aktivieren Sie das Kontrollkästchen „Windows-Authentifizierung“.
- 4 Klicken Sie auf **Speichern**.
- 5 Führen Sie die Voraussetzungsprüfung erneut aus.

Model Manager-Daten und Webkomponenten können nicht installiert werden

Ihre vRealize Automation-Installation schlägt möglicherweise fehl, wenn das IaaS-Installationsprogramm die Model Manager-Datenkomponente und die Webkomponente nicht speichern kann.

Problem

Die Installation schlägt mit folgender Meldung fehl:

Das IaaS-Installationsprogramm konnte die Model Manager-Daten und Webkomponenten nicht speichern.

Ursache

Der Fehler kann mehrere Ursachen haben.

- Probleme mit der Konnektivität zur vRealize Automation-Appliance oder Konnektivitätsprobleme zwischen den Appliances. Ein Verbindungsversuch ist fehlgeschlagen, da keine Antwort erhalten wurde oder die Verbindung nicht hergestellt werden konnte.
- Probleme mit vertrauenswürdigen Zertifikaten in IaaS bei Verwendung einer verteilten Konfiguration.
- Ein Zertifikatnamenskonflikt in einer verteilten Konfiguration.
- Möglicherweise ist das Zertifikat ungültig oder in der Zertifikatskette ist ein Fehler vorhanden.
- Der Repository-Dienst kann nicht gestartet werden.
- Eine nicht ordnungsgemäße Konfiguration des Lastausgleichsdiensts in einer verteilten Umgebung.

Lösung

- Konnektivität

Stellen Sie sicher, dass Sie eine Verbindung zur vRealize Automation-URL in einem Webbrowser herstellen können.

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

- Probleme mit vertrauenswürdigen Zertifikaten

- Öffnen Sie mit dem Befehl `mmc . exe` Microsoft Management Console in IaaS und überprüfen Sie, ob das in der Installation verwendete Zertifikat zum Zertifikatspeicher für vertrauenswürdige Stammzertifikate in der Maschine hinzugefügt wurde.

- Überprüfen Sie in einem Webbrowser den Status des MetaModel-Diensts und vergewissern Sie sich, dass kein Zertifikatsfehler angezeigt wird:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

- **Zertifikatnamenskonflikt**

Dieser Fehler kann auftreten, wenn das Zertifikat für einen bestimmten Namen ausgegeben wurde und ein anderer Name oder eine andere IP-Adresse verwendet wird. Sie können den Fehler bei Zertifikatnamenskonflikten während der Installation unterdrücken, indem Sie **Zertifikatkonflikt unterdrücken** auswählen.

Sie können die Option zur Unterdrückung des Zertifikatkonflikts auch verwenden, um Fehler bei Konflikten mit Remote-Zertifikatsperrlisten zu ignorieren.

- **Ungültiges Zertifikat**

Öffnen Sie Microsoft Management Console mit dem Befehl `mmc .exe`. Stellen Sie sicher, dass das Zertifikat nicht abgelaufen und der Status korrekt ist. Führen Sie dies für alle Zertifikate in der Zertifikatskette durch. Möglicherweise müssen Sie andere Zertifikate in der Kette in den Zertifikatspeicher für vertrauenswürdige Stammzertifikate importieren, wenn Sie eine Zertifikatshierarchie verwenden.

- **Repository-Dienst**

Führen Sie folgende Aktionen durch, um den Status des Repository-Diensts zu überprüfen.

- Überprüfen Sie in einem Webbrowser den Status des MetaModel-Diensts:
`https://FQDN-or-IP/repository/data/MetaModel.svc`
- Überprüfen Sie das `Repository.log` auf Fehler.
- Setzen Sie IIS (`iisreset`) zurück, wenn Sie Probleme mit den auf der Website gehosteten Anwendungen haben (Repository, vRealize Automation oder WAPI).
- Weitere Protokollierungsinformationen finden Sie in den Website-Protokollen unter `%System-Drive%\inetpub\logs\LogFiles`.
- Stellen Sie sicher, dass die Voraussetzungsprüfung bei der Überprüfung der Anforderungen bestanden wurde.
- Stellen Sie bei Windows 2012 sicher, dass die WCF-Dienste unter .NET Framework installiert sind und dass die HTTP-Aktivierung installiert ist.

IaaS -Windows-Server unterstützen kein FIPS

Eine Installation kann nicht erfolgreich abgeschlossen werden, wenn FIPS (Federal Information Processing Standard) aktiviert ist.

Problem

Die Installation schlägt beim Installieren der IaaS-Webkomponenten mit dem folgenden Fehler fehl.

Diese Implementierung ist nicht Teil der durch FIPS für Windows-Plattformen validierten kryptografischen Algorithmen.

Ursache

vRealize Automation IaaS basiert auf Microsoft Windows Communication Foundation (WCF), und FIPS wird daher nicht unterstützt.

Lösung

Deaktivieren Sie auf dem IaaS-Windows-Server die FIPS-Richtlinie.

- 1 Wechseln Sie zu **Start > Systemsteuerung > Verwaltung > Lokale Sicherheitsrichtlinie**.
- 2 Wählen Sie im Dialogfeld „Gruppenrichtlinie“ unter **Lokale Richtlinien** die Option **Sicherheitsoptionen** aus.
- 3 Suchen Sie den folgenden Eintrag und deaktivieren Sie ihn:
Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden.

Interner Fehler durch Hinzufügen eines XaaS -Endpoints

Beim Versuch, einen XaaS-Endpoint zu erstellen, wird eine interne Fehlermeldung angezeigt.

Problem

Die Erstellung eines Endpoints schlägt mit der folgenden internen Fehlermeldung fehl: Ein interner Fehler ist aufgetreten. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Systemadministrator. Dabei geben Sie ihm folgende Referenz bekannt: `c0DD0C01`. Referenzcodes werden nach dem Zufallsprinzip generiert und sind nicht mit einer bestimmten Fehlermeldung verknüpft.

Lösung

- 1 Öffnen Sie die Protokolldatei für die vRealize Automation-Appliance.
`/var/log/vcac/catalina.out`
- 2 Suchen Sie in der Fehlermeldung nach dem Referenzcode.
Beispielsweise `c0DD0C01`.
- 3 Suchen Sie in der Protokolldatei nach dem Referenzcode, um den zugehörigen Eintrag aufzufinden.
- 4 Überprüfen Sie die Einträge, die über und unter dem zugehörigen Eintrag angezeigt werden, um eine Fehlerbehebung des Problems vorzunehmen.

Der zugehörige Protokolleintrag verweist nicht spezifisch auf die Ursache des Problems.

Ein Proxy-Agent kann nicht deinstalliert werden

Das Entfernen eines Proxy-Agents kann fehlschlagen, wenn die Windows Installer-Protokollierung aktiviert ist.

Problem

Wenn Sie versuchen, einen Proxy-Agent von der Windows-Systemsteuerung zu deinstallieren, schlägt die Deinstallation fehl und die folgende Fehlermeldung wird angezeigt:

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

Ursache

Dies kann auftreten, wenn die Windows Installer-Protokollierung aktiviert ist, aber die Windows Installer-Engine kann die Deinstallations-Protokolldatei nicht ordnungsgemäß schreiben. Weitere Informationen finden Sie im [Microsoft Knowledgebase-Artikel 2564571](#).

Lösung

- 1 Starten Sie die Maschine neu oder starten Sie explorer.exe über den Task-Manager neu.
- 2 Deinstallieren Sie den Agent.

Fehler bei Maschinenanforderungen, wenn Remote-Transaktionen deaktiviert sind

Es kommt zu einem Fehler bei Maschinenanforderungen, wenn DTC-Remote-Transaktionen (Microsoft Distributed Transaction Coordinator) auf Windows-Server-Maschinen deaktiviert sind.

Problem

Wenn Sie eine Maschine bereitstellen, wenn Remote-Transaktionen auf dem Model Manager-Portal oder dem SQL Server deaktiviert sind, wird die Anforderung nicht abgeschlossen. Es kommt zu einem Fehler bei der Datenerfassung, und die Maschinenanforderung verbleibt in einem Status für den Klonworkflow.

Ursache

DTC-Remote-Transaktionen sind in der IaaS-SQL-Instanz deaktiviert, die von dem vRealize Automation-System verwendet wird.

Lösung

- 1 Starten Sie Windows Server Manager zum Aktivieren von DTC auf allen vRealize-Servern und zugeordneten SQL-Servern.

Navigieren Sie in Windows 7 zu **Start > Verwaltungstools > Komponentendienste**.

Hinweis Stellen Sie sicher, dass alle Windows-Server über eindeutige SIDs für die MSDTC-Konfiguration verfügen.

Darüber hinaus muss der IaaS Manager Service-Host den NetBIOS-Namen des IaaS-SQL-Server-Datenbankhosts auflösen können. Wenn er den NetBIOS-Namen nicht auflösen kann, fügen Sie der Datei /etc/hosts der Manager Service-Maschine den NetBIOS-Namen des SQL-Servers hinzu und starten Sie den Manager Service neu.

- 2 Öffnen Sie alle Knoten zum Suchen des lokalen DTC oder den geclusterten DTC bei Verwendung eines geclusterten Systems.

Navigieren Sie zu **Komponentendienste > Computer > Mein Computer > Distributed Transaction Coordinator**.

- 3 Klicken Sie mit der rechten Maustaste auf den lokalen oder geclusterten DTC und wählen Sie **Eigenschaften** aus.
- 4 Klicken Sie auf die Registerkarte „Sicherheit“.
- 5 Wählen Sie die Option **DTC-Netzwerkzugriff** aus.

- 6 Wählen Sie die Optionen **Remote-Client zulassen** und **Remoteverwaltung zulassen** aus.
- 7 Wählen Sie die Optionen **Eingehende zulassen** und **Ausgehende zulassen** aus.
- 8 Geben Sie NT AUTHORITY\Network Service in das Feld **Konto** für das DTC-Anmeldekonto ein bzw. wählen Sie es aus.
- 9 Klicken Sie auf **OK**.
- 10 Entfernen Sie Maschinen, die im Status für den Klonworkflow hängen geblieben sind.
 - a Melden Sie sich bei der Produktschnittstelle von vRealize Automation an.
`https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name`
 - b Navigieren Sie zu **Infrastruktur > Verwaltete Maschinen**.
 - c Klicken Sie mit der rechten Maustaste auf die Zielmaschine.
 - d Wählen Sie **Löschen** zum Entfernen der Maschine aus.

Fehler bei der Kommunikation mit dem Manager Service

IaaS-Server, die über eine Vorlage mit bereits installiertem DTC geklont werden, enthalten duplizierte Bezeichner für DTC, wodurch die Kommunikation zwischen den Knoten verhindert wird.

Problem

Der IaaS Manager Service schlägt fehl, und es wird die folgende Fehlermeldung im Manager Service-Protokoll veröffentlicht.

```
Fehler bei der Kommunikation mit dem zugrunde liegenden Transaktions-Manager. ---> System.Runtime.InteropServices.COMException: Aufgrund von Kommunikationsproblemen konnte der MSDTC-Transaktions-Manager die Transaktion nicht vom Quelltransaktions-Manager übernehmen. Mögliche Ursachen: Es ist eine Firewall vorhanden, für die für den MSDTC-Prozess keine Ausnahme festgelegt wurde, die Computer können sich nicht anhand ihrer NetBIOS-Namen finden, oder die Unterstützung von Netzwerktransaktionen ist für einen der beiden Transaktions-Manager nicht aktiviert.
```

Ursache

Wenn Sie einen IaaS-Server klonen, auf dem DTC bereits installiert ist, enthält der Klon denselben eindeutigen Bezeichner für DTC wie das übergeordnete Element. Die Kommunikation zwischen den beiden Maschinen schlägt fehl.

Lösung

- 1 Öffnen Sie auf dem Klon eine Eingabeaufforderung als Administrator.
- 2 Führen Sie folgenden Befehl aus.
`msdtc -uninstall`
- 3 Starten Sie den Klon neu.
- 4 Öffnen Sie eine weitere Eingabeaufforderung und führen Sie den folgenden Befehl aus.
`msdtc -install manager-service-host-FQDN`

Geändertes Verhalten für die Anpassung von E-Mails

In vRealize Automation 6.0 oder höher können nur die von der IaaS-Komponente generierten Benachrichtigungen mithilfe der E-Mail-Vorlagenfunktion aus früheren Versionen angepasst werden.

Lösung

Sie können die folgenden XSLT-Vorlagen verwenden:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

E-Mail-Vorlagen sind im Verzeichnis `\Templates` des Serverinstallationsverzeichnis gespeichert, in der Regel `%SystemDrive%\Programme (x86)\VMware\vCAC\Server`. Das Verzeichnis `\Templates` enthält auch XSLT-Vorlagen, die nicht mehr unterstützt werden und nicht geändert werden können.

Fehlerbehebung bei Anmeldefehlern

Die Themen zur Fehlerbehebung bei Anmeldefehlern für vRealize Automation liefern Lösungen für potenzielle Probleme im Zusammenhang mit der Installation, die bei der Verwendung von vRealize Automation auftreten können.

Anmeldeversuche als IaaS-Administrator mit falsch formatierten UPN-Anmeldedaten schlagen ohne Begründung fehl

Sie versuchen, sich bei vRealize Automation als IaaS-Administrator anzumelden und werden ohne Begründung an die Anmeldeseite weitergeleitet.

Problem

Wenn Sie versuchen, sich bei vRealize Automation als IaaS-Administrator mit UPN-Anmeldedaten ohne die Komponente `"@IhreDomäne"` des Benutzernamens anzumelden, werden Sie von SSO sofort abgemeldet und ohne Begründung an die Anmeldeseite umgeleitet.

Ursache

Der eingegebene UPN muss das Format *IhrName.admin@IhreDomäne* aufweisen. Wenn Sie sich beispielsweise mit *jsmith.admin@sqa.local* als Benutzername anmelden, aber der UPN in Active Directory nur als *jsmith.admin* festgelegt ist, schlägt die Anmeldung fehl.

Lösung

Um dieses Problem zu beheben, ändern Sie den Wert `userPrincipalName` und fügen den erforderlichen Inhalt *@IhreDomäne* hinzu. Anschließend melden Sie sich erneut an. In diesem Beispiel sollte der UPN-Name „*jsmith.admin@sqa.local*“ lauten. Diese Informationen finden Sie in der Protokolldatei im Ordner `Log/vcac`.

Anmeldung schlägt fehl bei Hochverfügbarkeit

Wenn Sie über mehrere vRealize Automation-Appliances verfügen, müssen sich die Appliances gegenseitig anhand eines kurzen Hostnamens identifizieren können. Andernfalls können Sie sich nicht anmelden.

Problem

Sie konfigurieren vRealize Automation für Hochverfügbarkeit durch Installation einer zusätzlichen vRealize Automation-Appliance. Wenn Sie versuchen, sich bei vRealize Automation anzumelden, wird eine Meldung über eine ungültige Lizenz angezeigt. Die Meldung ist jedoch falsch, da Sie ermittelt haben, dass Ihre Lizenz gültig ist.

Ursache

Die vRealize Automation-Appliance-Knoten bilden erst dann ordnungsgemäß einen Hochverfügbarkeitscluster, wenn sie die kurzen Hostnamen der Knoten im Cluster auflösen können.

Lösung

Damit ein Cluster mit hochverfügbaren vRealize Automation-Appliances kurze Hostnamen auflösen kann, führen Sie eines der folgenden Verfahren durch. Sie müssen alle Appliances im Cluster ändern.

Verfahren

- Bearbeiten oder erstellen Sie eine Suchzeile in der Datei `/etc/resolv.conf`. Die Zeile sollte Domänen enthalten, die vRealize Automation-Appliances beinhalten. Trennen Sie mehrere Domänen durch Leerzeichen. Beispiel:

```
search sales.mycompany.com support.mycompany.com
```

- Bearbeiten oder erstellen Sie Domänenzeilen in der Datei `/etc/resolv.conf`. Jede Zeile sollte eine Domäne enthalten, die vRealize Automation-Appliances beinhaltet. Beispiel:

```
domain support.mycompany.com
```

- Fügen Sie der Datei `/etc/hosts` Zeilen hinzu, sodass jeder Kurzname einer vRealize Automation-Appliance ihrem vollqualifizierten Domännennamen zugeordnet wird. Beispiel:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

Proxy verhindert VMware Identity Manager -Benutzeranmeldung

Wenn Sie die Verwendung eines Proxyservers konfigurieren, wird möglicherweise die Anmeldung von VMware Identity Manager-Benutzern verhindert.

Problem

Sie konfigurieren für vRealize Automation den Zugriff auf das Netzwerk über einen Proxyserver und VMware Identity Manager-Benutzern wird beim Anmelden folgende Fehlermeldung angezeigt.

```
Error Unable to get metadata
```

Lösung

Voraussetzungen

Konfigurieren Sie vRealize Automation für den Zugriff auf das Netzwerk über einen Proxyserver. Siehe [Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server](#).

Verfahren

- 1 Melden Sie sich bei der Konsole der vRealize Automation-Appliance als Root-Benutzer an.
- 2 Öffnen Sie die folgende Datei in einem Texteditor.
`/etc/sysconfig/proxy`
- 3 Aktualisieren Sie die Zeile `NO_PROXY`, um den Proxyserver für VMware Identity Manager-Anmeldungen zu ignorieren.

```
NO_PROXY=vrealize-automation-hostname
```

```
Beispiel: NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"
```

- 4 Speichern und schließen Sie `proxy`.
- 5 Starten Sie den Horizon Workspace-Dienst neu, indem Sie den folgenden Befehl eingeben.

```
service horizon-workspace restart
```

Aktualisieren von vRealize Automation

Sie können ein Upgrade Ihrer aktuellen vRealize Automation-Umgebung auf die neueste Version durchführen.

Abhängig von Ihrer aktuellen vRealize Automation-Umgebung können Sie auf die neueste Version aktualisieren, indem Sie ein direktes Upgrade oder ein Side-by-Side-Upgrade durchführen. Prüfen Sie die Informationen auf dieser Seite, um die beste Upgrade-Methode für Ihre Umgebung zu ermitteln.

Ein direktes Upgrade besteht aus mehreren Schritten. Sie führen Prozeduren in einer bestimmten Reihenfolge aus, um die verschiedenen Komponenten in Ihrer aktuellen Umgebung zu aktualisieren. Sie müssen bei allen Produktkomponenten ein Upgrade auf dieselbe Version durchführen. Sie können nur ein direktes Upgrade für diese Pfade durchführen.

- vRealize Automation 6.2.5 auf 7.4
- vRealize Automation 7.1 auf 7.4
- vRealize Automation 7.2 auf 7.4
- vRealize Automation 7.3.x auf 7.4

Bei einem parallelen Upgrade werden Daten in Ihrer aktuellen vRealize Automation-Umgebung zu einer Zielumgebung migriert, die mit der aktuellen Version von vRealize Automation bereitgestellt wird. Sie können ein paralleles Upgrade für diese Pfade durchführen.

- vRealize Automation 6.2.0 über 6.2.5 auf 7.4
- vRealize Automation 7.0 und 7.0.1 auf 7.4
- vRealize Automation 7.1, 7.2 und 7.3.x auf 7.4

Bei der Migration wird Ihre aktuelle Umgebung nicht geändert. Wenn Ihre aktuelle Umgebung in vCloud Director oder vCloud Air integriert ist oder physische Endpoints aufweist, müssen Sie mithilfe der Migration ein Upgrade durchführen. Im Rahmen der Migration werden alle nicht unterstützten Endpoints und alle damit verknüpften Elemente in der Zielumgebung entfernt.

Suchen Sie Ihre aktuelle vRealize Automation-Version in dieser Tabelle. Verwenden Sie die Dokumente rechts, um ein Upgrade Ihrer vRealize Automation-Umgebung auf die neueste Version durchzuführen.

Tabelle 1-45. Unterstützte Upgrade-Pfade auf vRealize Automation 7.4

Aktuell installierte Version	Dokumentation für inkrementelle Updates
vRealize Automation 7.1, 7.2 oder 7.3.x	Siehe eines dieser Themen. <ul style="list-style-type: none"> ■ Upgrade von vRealize Automation 7.1 oder höher auf 7.4 ■ Migrieren auf vRealize Automation 7.4
vRealize Automation 7.0 oder 7.0.1	Siehe Migrieren auf vRealize Automation 7.4 .
vRealize Automation 6.2.5	Siehe eines dieser Themen. <ul style="list-style-type: none"> ■ Upgrade von vRealize Automation 6.2.5 auf 7.4 ■ Migrieren auf vRealize Automation 7.4
vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4	Siehe Migrieren auf vRealize Automation 7.4 .

Diese Tabelle enthält Informationen zum Upgrade von einer früheren vCloud Automation Center-Version. Sie müssen vor dem Upgrade auf die neueste Version von vRealize Automation ein Upgrade auf vRealize Automation 6.2.5 durchführen. Links zur Dokumentation für 5.x- und 6.x-Versionen von vCloud Automation Center und vRealize Automation finden Sie unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Tabelle 1-46. Unterstützte Upgrade-Pfade auf vRealize Automation 6.2.5

Aktuell installierte Version	Dokumentation für inkrementelle Updates
vCloud Automation Center 6.0	Führen Sie die Upgrades in folgender Reihenfolge durch: 1 <i>Upgrade von vCloud Automation Center 6.0 auf 6.0.1</i> 2 <i>Upgrade auf vCloud Automation Center 6.1</i> 3 <i>Aktualisieren auf vRealize Automation 6.2.x</i>
vCloud Automation Center 6.0.1	Führen Sie die Upgrades in folgender Reihenfolge durch: 1 <i>Upgrade auf vCloud Automation Center 6.1</i> 2 <i>Aktualisieren auf vRealize Automation 6.2.x</i>
vCloud Automation Center 6.1.x	<i>Aktualisieren auf vRealize Automation 6.2.x</i>
vRealize Automation 6.2.x	Direktes Upgrade auf Version 6.2.5, wie unter <i>Aktualisieren auf vRealize Automation 6.2.x</i> beschrieben.

Hinweis vCloud Automation Center wurde in 6.2.0 in vRealize Automation umbenannt. Nur die Benutzeroberflächen- und Dienstnamen wurden geändert. Verzeichnisnamen und Programmnamen, die `vcac` enthalten, sind davon nicht betroffen.

Wenn Sie von einer 6.2.x-Umgebung aus aktualisieren, prüfen Sie folgende Elemente.

- Das VMware vRealize Production Test Upgrade Assessment-Tool analysiert Ihre vRealize Automation 6.2.x-Umgebung hinsichtlich jeder Funktionskonfiguration, die Upgrade-Probleme verursachen kann, und überprüft, ob Ihre Umgebung für das Upgrade bereit ist. Um dieses Tool und die zugehörige Dokumentation herunterzuladen, navigieren Sie zur Downloadseite für das [VMware vRealize Production Test Tool](#).
- Das Upgrade von einer 6.2.x-Umgebung auf die neueste Version von vRealize Automation umfasst zahlreiche funktionale Änderungen. Weitere Informationen finden Sie unter [Überlegungen zum Upgrade auf diese vRealize Automation-Version](#).
- Falls Sie Ihre vRealize Automation 6.2.x-Bereitstellung angepasst haben, wenden Sie sich wegen zusätzlicher Informationen zu Aktualisierungsaspekten an die Mitarbeiter des CCE-Supports.
- Steuerelemente von Eigenschaftenwörterbüchern, die nach dem Upgrade nicht unterstützt werden, können mithilfe von vRealize Orchestrator und Beziehungen von Eigenschaftenwörterbüchern wiederhergestellt werden.
- Wenn Ihre Quellumgebung Workflows mit veraltetem Code enthält, erhalten Sie Informationen zu Codeänderungen, die für die Umwandlung in Ereignisbrokerabonnements notwendig sind, im [vRealize Automation Extensibility Migration Guide](#).

Um ein bekanntes Problem bei der Aktualisierung von vRealize Automation 6.2.0 zu vermeiden, führen Sie die folgenden Schritte für jeden IaaS-Websiteknoten aus, bevor Sie das Upgrade durchführen. Dieses Problem betrifft nur Version 6.2.0. Andere 6.2.x-Versionen sind nicht davon betroffen.

- 1 Öffnen Sie den Editor mit Administratorrechten. Klicken Sie im Startmenü mit der rechten Maustaste auf das Editorsymbol und wählen Sie dann **Als Administrator ausführen** aus.
- 2 Öffnen Sie folgende Datei:

C:\Programme (x86)\VMware\vCAC\Server\Model Manager Web\Logs

- 3 Suchen Sie in der Datei nach der folgenden Anweisung:

```
<!-- add key="DisableMessageSignatureCheck" value="false"-->
```

- 4 Heben Sie den Kommentar der Anweisung auf und ändern Sie den Wert von `false` zu `true`.

```
<add key="DisableMessageSignatureCheck" value="true" />
```

- 5 Speichern Sie die Datei.

Wenn Sie im Editor zum Speichern unter aufgefordert werden, haben Sie den Editor nicht als Administrator geöffnet und müssen zu Schritt 1 zurückkehren.

- 6 Öffnen Sie die Eingabeaufforderung mit Administratorrechten. Klicken Sie im Startmenü mit der rechten Maustaste auf das Symbol „Eingabeaufforderung“ und wählen Sie **Als Administrator ausführen** aus.

- 7 Führen Sie „reset“ aus.

- 8 Wiederholen Sie die Schritte 1 bis 7 für alle Websiteknoten.

Upgrade von vRealize Automation 7.1 oder höher auf 7.4

Bei einem Upgrade Ihrer Umgebung mit vRealize Automation 7.1 oder höher auf die neueste Version verwenden Sie die Upgrade-Verfahren für Ihre Umgebung der Version 7.1 oder höher.

Diese Informationen gelten für das Upgrade von vRealize Automation 7.1 oder höher auf 7.4. Informationen zu anderen unterstützten Upgrade-Pfaden finden Sie unter [Aktualisieren von vRealize Automation](#).

Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4

Sie können ein Upgrade Ihrer aktuellen vRealize Automation 7.1-, 7.2- oder 7.3.x-Umgebung auf 7.4 durchführen. Für das Upgrade Ihrer Umgebung verwenden Sie die für diese Version spezifischen Upgrade-Verfahren.

Ein direktes Upgrade ist ein aus drei Stufen bestehendes Verfahren. Sie können die Komponenten in Ihrer aktuellen Umgebung in dieser Reihenfolge aktualisieren.

- 1 vRealize Automation-Appliance
- 2 IaaS-Webserver
- 3 vRealize Orchestrator

Sie müssen bei allen Produktkomponenten ein Upgrade auf dieselbe Version durchführen.

Ab vRealize Automation 7.2 wird JFrog Artifactory Pro nicht mehr im Paket mit der vRealize Automation-Appliance angeboten. Wenn Sie ein Upgrade von einer früheren Version von vRealize Automation durchführen, wird JFrog Artifactory Pro während des Upgradevorgangs entfernt. Weitere Informationen finden Sie im [Knowledgebase-Artikel 2147237](#).

Voraussetzungen für das Aktualisieren von vRealize Automation

Überprüfen Sie vor dem Upgrade Ihrer vRealize Automation 7.1-, 7.2- oder 7.3.x-Umgebung auf 7.4 die folgenden Voraussetzungen.

Systemkonfigurationsanforderungen

Stellen Sie vor dem Beginn einer Aktualisierung sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Stellen Sie sicher, dass alle Appliances und Server, die Teil der Bereitstellung sind, die Systemanforderungen für die neueste Version erfüllen. Weitere Informationen finden Sie unter *vRealize AutomationSupport-Matrix* in der [VMware vRealize Automation-Dokumentation](#).
- In der *VMware Product Interoperability Matrix* auf der VMware-Website finden Sie Informationen über die Kompatibilität mit anderen VMware-Produkten.
- Stellen Sie sicher, dass es sich bei der vRealize Automation-Version, von der aus Sie das Upgrade durchführen, um eine stabile Version handelt. Korrigieren Sie etwaige Probleme vor der Durchführung des Upgrades.
- Vergewissern Sie sich, dass Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst vom Standardwert auf mindestens 10 Minuten geändert haben.

Hardwarekonfigurationsanforderungen

Vergewissern Sie sich, dass die Hardware in Ihrer Umgebung für vRealize Automation 7.4 geeignet ist.

Siehe [vRealize Automation-Hardware-Spezifikationen und maximale Kapazitäten](#).

Stellen Sie vor dem Beginn einer Aktualisierung sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Sie müssen mindestens über 18 GB RAM, 4 CPUs, Disk1 = 50 GB, Disk3=25 GB und Disk4=50 GB verfügen, bevor Sie das Upgrade ausführen können.

Wenn die virtuelle Maschine unter vCloud Networking and Security ausgeführt wird, müssen Sie möglicherweise mehr RAM-Speicher zuteilen.

Obwohl die allgemeine Unterstützung für vCloud Networking and Security beendet wurde, sind die benutzerdefinierten VCNS-Eigenschaften nach wie vor zu NSX-Zwecken gültig. Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2144733](#).

- Die folgenden Knoten müssen mindestens über 5 GB freien Festplattenspeicher verfügen:
 - Primäre IaaS-Website
 - Microsoft SQL-Datenbank
 - Model Manager
- Der primäre IaaS-Websiteknoten, auf dem die Model Manager-Daten installiert sind, muss über JAVA SE Runtime Environment 8, 64 Bit, Update 161 oder höher verfügen. Nach der Installation von Java müssen Sie die Umgebungsvariable JAVA_HOME auf die neue Version aktualisieren.
- Um das Upgrade herunterzuladen und auszuführen, benötigen Sie die folgenden Ressourcen:
 - Mindestens 5 GB auf der Root-Partition
 - 5 GB auf der Partition `/storage/db` für die Master-vRealize Automation-Appliance
 - 5 GB auf der Root-Partition für jede virtuelle Replikat-Appliance
- Öffnen Sie den Unterordner `/storage/log` und entfernen Sie alle älteren archivierten ZIP-Dateien, um Speicherplatz zu bereinigen.

Allgemeine Voraussetzungen

Stellen Sie vor dem Beginn einer Aktualisierung sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Vor dem Upgrade müssen Sie PowerShell 3.0 oder höher auf Ihren Windows-IaaS-Systemen installieren. Das Upgrade schlägt fehl, wenn PowerShell 3.0 oder höher nicht installiert ist.
- Führen Sie ein IISRESET auf Ihren IaaS Web- und IaaS Manager Service-Maschinen aus, wenn Microsoft IIS installiert ist. Mit dem Ausführen von IISRESET wird sichergestellt, dass kein von IIS abhängiger deaktivierter Dienst im Startmodus vorhanden ist.
- Sie haben Zugriff auf alle Datenbanken und alle Lastausgleichsdienste, die von dem Upgrade für vRealize Automation betroffen sind oder daran beteiligt sind.
- Während der Durchführung des Upgrades ist das System für Benutzer nicht verfügbar.
- Sie deaktivieren alle Anwendungen, die vRealize Automation abfragen.
- Stellen Sie sicher, Microsoft Distributed Transaction Coordinator (MSDTC) auf allen vRealize Automation- und zugehörigen SQL-Servern aktiviert ist. Weitere Anweisungen finden Sie im [Knowledgebase-Artikel 2089503](#).
- Führen Sie diese Schritte aus, wenn Sie eine verteilte Umgebung aktualisieren, die mit einer eingebetteten PostgreSQL-Datenbank konfiguriert wurde.
 - a Überprüfen Sie die Dateien im Verzeichnis `pgdata` auf dem Master-Host, bevor Sie die Replikat-Hosts aktualisieren.
 - b Navigieren Sie zum PostgreSQL-Datenordner auf dem Master-Host unter `/var/vmware/vpostgres/current/pgdata/`.
 - c Schließen Sie alle geöffneten Dateien im Verzeichnis `pgdata` und entfernen Sie alle Dateien mit dem Suffix „.swp“.
 - d Stellen Sie sicher, dass alle Dateien in diesem Verzeichnis über den richtigen Besitzer verfügen: `postgres:users`.

Stellen Sie darüber hinaus sicher, dass benutzerdefinierte Eigenschaften keine Leerzeichen im Namen haben. Entfernen Sie vor dem Upgrade auf diese Version von vRealize Automation alle Leerzeichen aus Ihren benutzerdefinierten Eigenschaftsnamen. Ersetzen Sie z. B. das Leerzeichen durch einen Unterstrich, damit die benutzerdefinierte Eigenschaft in der aktualisierten vRealize Automation-Installation erkannt werden kann. Namen benutzerdefinierter Eigenschaften in vRealize Automation dürfen keine Leerzeichen enthalten. Dieses Problem kann sich auf die Verwendung einer aktualisierten vRealize Orchestrator-Installation auswirken, die benutzerdefinierte Eigenschaften verwendet, welche in früheren Versionen von vRealize Automation oder vRealize Orchestrator oder beidem Leerzeichen enthielten.

Checkliste für das Upgrade von vRealize Automation

Wenn Sie ein Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 durchführen, aktualisieren Sie alle vRealize Automation-Komponenten in einer bestimmten Reihenfolge.

Die Upgrade-Reihenfolge variiert, je nachdem, ob Sie ein Upgrade für eine Minimalumgebung oder eine verteilte Umgebung mit mehreren vRealize Automation-Appliances durchführen.

Verwenden Sie die Checklisten, um Ihre Arbeit beim Durchführen des Upgrades zu verfolgen. Führen Sie die Aufgaben in der Reihenfolge aus, in der sie vorgegeben werden.

Tabelle 1-47. Checkliste für das Upgrade von einer minimalen vRealize Automation - Umgebung

Aufgabe	Anleitung
<input type="checkbox"/> Führen Sie vor dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste aus. Dieser Schritt ist nur erforderlich, wenn vRealize Automation in NSX integriert ist.	Siehe Durchführen der Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste vor dem vRealize Automation-Upgrade .
<input type="checkbox"/> Sichern Sie Ihre aktuelle Installation. Dies ist ein wesentlicher Schritt.	Weitere Informationen zum Sichern und Wiederherstellen des Systems finden Sie unter Sichern Ihrer vorhandenen vRealize Automation-Umgebung . Allgemeine Informationen finden Sie im Dokument <i>Configuring Backup and Restore by Using Symantec Netbackup</i> (Konfigurieren der Sicherung und Wiederherstellung unter Verwendung von Symantec Netbackup) unter der Adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-net-backup.pdf .
<input type="checkbox"/> Laden Sie das Update für die vRealize Automation-Appliance herunter.	Siehe Herunterladen von Updates für vRealize Automation-Appliances .
<input type="checkbox"/> Installieren Sie das Update auf der vRealize Automation-Appliance und den IaaS-Komponenten.	Siehe Installieren des Updates auf der vRealize Automation-Appliance und den IaaS-Komponenten .

Tabelle 1-48. Checkliste für das Upgrade einer verteilten vRealize Automation -Umgebung

Aufgabe	Anleitung
<input type="checkbox"/> Führen Sie vor dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 aus. Dieser Schritt ist nur erforderlich, wenn vRealize Automation in NSX integriert ist.	Siehe Durchführen der Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste vor dem vRealize Automation-Upgrade .
<input type="checkbox"/> Sichern Sie Ihre aktuelle Installation. Dies ist ein wesentlicher Schritt.	Weitere Informationen zum Sichern und Wiederherstellen des Systems finden Sie unter Sichern Ihrer vorhandenen vRealize Automation-Umgebung . Detaillierte Informationen finden Sie im Dokument <i>Configuring Backup and Restore by Using Symantec Netbackup</i> (Konfigurieren der Sicherung und Wiederherstellung unter Verwendung von Symantec Netbackup) unter der Adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-net-backup.pdf .
<input type="checkbox"/> Wenn Sie ein Upgrade von vRealize Automation 7.3.x durchführen, deaktivieren Sie das automatische Failover von PostgreSQL.	Siehe Festlegen des vRealize Automation PostgreSQL-Replikatmodus auf „asynchron“ .

Tabelle 1-48. Checkliste für das Upgrade einer verteilten vRealize Automation -Umgebung (Fortsetzung)

Aufgabe	Anleitung
<input type="checkbox"/> Laden Sie Updates für die vRealize Automation-Appliance herunter.	Siehe Herunterladen von Updates für vRealize Automation-Appliances .
<input type="checkbox"/> Deaktivieren Sie den Lastausgleich.	Weitere Informationen finden Sie in der Dokumentation des Lastausgleichs.
<input type="checkbox"/> Installieren Sie das Update auf der vRealize Automation-Master-Appliance und den IaaS-Komponenten.	Siehe Installieren des Updates auf der vRealize Automation-Appliance und den IaaS-Komponenten .
Hinweis Sie müssen das Update auf der Master-Appliance in einer verteilten Umgebung installieren.	
<input type="checkbox"/> Aktivieren Sie den Lastausgleich.	Aktivieren der Lastausgleichsdienste

Benutzeroberflächen der vRealize Automation -Umgebung

Sie verwenden und verwalten Ihre vRealize Automation-Umgebung mit mehreren Schnittstellen.

Benutzeroberfläche

In diesen Tabellen werden die Schnittstellen beschrieben, die Sie zum Verwalten Ihrer vRealize Automation-Umgebung verwenden

Tabelle 1-49. vRealize Automation Verwaltungskonsole

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die vRealize Automation-Konsole für diese Systemadministrationsaufgaben.</p> <ul style="list-style-type: none"> ■ Mandanten hinzufügen. ■ vRealize Automation-Benutzeroberfläche anpassen. ■ E-Mail-Server konfigurieren. ■ Ereignisprotokolle anzeigen. ■ Konfigurieren Sie vRealize Orchestrator. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf vRealize Automation-Konsole. Sie können auch diese URL zum Öffnen der vRealize Automation-Konsole verwenden: <code>https://vra-va-hostname.domain.name/vcac</code> 3 Melden Sie sich an. 	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle sein.</p>

Tabelle 1-50. vRealize Automation -Mandantenkonsole. Diese Schnittstelle ist die primäre Benutzeroberfläche, mit der Sie Ihre Dienste und Ressourcen erstellen und verwalten.

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden vRealize Automation für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Neue IT-Dienst-Blueprints anfordern. ■ Cloud- und IT-Ressourcen erstellen und verwalten. ■ Benutzerdefinierte Gruppen erstellen und verwalten. ■ Erstellt und verwaltet Business-Gruppen. ■ Rollen zu Benutzern zuweisen. 	<p>1 Starten Sie einen Browser und geben Sie die URL für Ihren Mandanten mit dem vollqualifizierten Domännennamen der virtuelle Appliance und dem Namen der Mandanten-URL ein.</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name .</code></p> <p>2 Melden Sie sich an.</p>	<p>Sie müssen ein Benutzer mit mindestens einer dieser Rollen sein:</p> <ul style="list-style-type: none"> ■ Anwendungsarchitekt ■ Genehmigungsadministrator ■ Katalog-Administrator ■ Container-Administrator ■ Container-Architekt ■ Health Consumer ■ Infrastrukturarchitekt ■ Sicherer Export, Verbraucher ■ Softwarearchitekt ■ Mandantenadministrator ■ XaaS-Architekt

Tabelle 1-51. Verwaltung der vRealize Automation -Appliance Diese Schnittstelle wird manchmal als „Virtual Appliance Management Interface“ (VAMI) bezeichnet.

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Verwaltung der vRealize Automation-Appliance für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Status der registrierte Dienste anzeigen. ■ Systeminformationen anzeigen und die Appliance neu starten oder herunterfahren. ■ Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit verwalten. ■ Netzwerkstatus anzeigen. ■ Updatestatus anzeigen und Updates installieren. ■ Administrationseinstellungen verwalten. ■ vRealize Automation-Hosteinstellungen verwalten. ■ SSO-Einstellungen verwalten. ■ Lizenzen verwalten. ■ vRealize Automation-Postgres-Datenbank konfigurieren. ■ vRealize Automation-Meldungen konfigurieren. ■ vRealize Automation-Protokollierung konfigurieren. ■ IaaS-Komponenten installieren. ■ Von einer vorhandenen vRealize Automation-Installation migrieren. ■ IaaS-Komponentenzertifikate verwalten. ■ Xenon-Dienst konfigurieren. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance. Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code> 3 Melden Sie sich an. 	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance eingegebene Kennwort.

Tabelle 1-52. vRealize Orchestrator -Client

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden den vRealize Orchestrator-Client für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Aktionen entwickeln. ■ Workflows entwickeln. ■ Richtlinien verwalten. ■ Pakete installieren. ■ Berechtigungen für Benutzer und Benutzergruppen verwalten. ■ Tags an URI-Objekte anhängen. ■ Bestandsliste anzeigen. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die vRealize Automation-Begrüßungsseite mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Um die Datei „client.jnlp“ auf Ihren lokalen Computer zu laden, klicken Sie auf vRealize Orchestrator-Client. 3 Klicken Sie mit der rechten Maustaste auf die <code>client.jnlp</code>-Datei und wählen Sie Starten aus. 4 Klicken Sie im Dialogfeld „Möchten Sie fortfahren“ auf Weiter. 5 Melden Sie sich an. 	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle oder Mitglied der Gruppe „vcoadmins“ in den Authentifizierungsanbieter-Einstellungen im vRealize Orchestrator-Control Center sein.</p>

Tabelle 1-53. vRealize Orchestrator Control Center

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden das vRealize Orchestrator Control Center, um die Konfiguration der vRealize Orchestrator-Standardinstanz zu bearbeiten, die in vRealize Automation eingebettet ist.</p>	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance. Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code> 3 Melden Sie sich an. 4 Klicken Sie auf vRA-Einstellungen > Orchestrator. 5 Wählen Sie Orchestrator-Benutzeroberfläche aus. 6 Klicken Sie auf Starten. 7 Klicken Sie auf die URL für die Orchestrator-Benutzeroberfläche. 8 Melden Sie sich an. 	<p>Benutzername</p> <ul style="list-style-type: none"> ■ Geben Sie root ein, wenn keine rollenbasierte Authentifizierung konfiguriert ist. ■ Geben Sie Ihren vRealize Automation-Benutzernamen ein, wenn dieser für die rollenbasierte Authentifizierung konfiguriert ist. <p>Kennwort</p> <ul style="list-style-type: none"> ■ Geben Sie das Kennwort ein, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben, wenn die rollenbasierte Authentifizierung nicht konfiguriert ist. ■ Geben Sie das Kennwort für Ihren Benutzernamen ein, wenn Ihr Benutzername für die rollenbasierte Authentifizierung konfiguriert ist.

Tabelle 1-54. Linux-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Linux-Befehlszeile auf einem Host, z. B. auf dem Host der vRealize Automation-Appliance Host, für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Dienste starten oder beenden ■ Konfigurationsdateien bearbeiten ■ Befehle ausführen ■ Daten abrufen 	<p>1 Öffnen Sie auf dem Host der vRealize Automation-Appliance eine neue Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile auf Ihrem lokalen Computer zu öffnen, ist das Starten einer Sitzung auf dem Host mit einer Anwendung, zum Beispiel PuTTY.</p> <p>2 Melden Sie sich an.</p>	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance erstellt Kennwort.

Tabelle 1-55. Windows-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Wie können eine Windows-Eingabeaufforderung auf einem Host verwenden z. B. auf dem IaaS-Host, um Skripts ausführen.</p>	<p>1 Melden Sie sich auf dem IaaS-Host bei Windows an.</p> <p>Eine Möglichkeit, sich über Ihren lokalen Computer anzumelden, ist das Starten einer Remote-Desktop-Sitzung.</p> <p>2 Öffnen Sie die Windows-Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile zu öffnen, ist das Klicken mit der rechten Maustaste auf das Startsymbol auf dem Host und die Auswahl von Eingabeaufforderung oder Eingabeaufforderung (Admin).</p>	<ul style="list-style-type: none"> ■ Benutzername: Benutzer mit Administratorrechten. ■ Kennwort: Kennwort des Benutzers.

Upgrade von in vRealize Automation integrierten VMware -Produkten

Beim Upgrade von vRealize Automation müssen Sie alle in Ihre vRealize Automation-Umgebung integrierten VMware-Produkte verwalten.

Wenn Ihre vRealize Automation-Umgebung in ein oder mehrere zusätzliche Produkte integriert ist, sollten Sie ein Upgrade von vRealize Automation vornehmen, bevor Sie zusätzliche Produkte aktualisieren.

Wenn vRealize Business for Cloud in vRealize Automation integriert ist, müssen Sie die Registrierung von vRealize Business for Cloud vor dem Upgrade von vRealize Automation aufheben.

Folgen Sie dem vorgeschlagenen Workflow für die Verwaltung von integrierten Produkten beim Upgrade von vRealize Automation.

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von VMware vRealize Operations Manager durch.
- 3 Führen Sie ein Upgrade von VMware vRealize Log Insight durch.
- 4 Führen Sie ein Upgrade von VMware vRealize Business for Cloud durch.

Dieser Abschnitt bietet zusätzliche Unterstützung für die Verwaltung von vRealize Business for Cloud bei Integration in Ihre vRealize Automation-Umgebung.

Upgrade von einer in vRealize Automation integrierten vRealize Operations Manager - Instanz

Führen Sie nach dem Upgrade von vRealize Automation ein Upgrade von vRealize Operations Manager aus.

Verfahren

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von vRealize Operations Manager durch. Informationen finden Sie unter *Aktualisieren Ihrer Software* in der [VMware vRealize Operations Manager-Dokumentation](#).

Upgrade von einer in vRealize Automation integrierten vRealize Log Insight -Instanz

Führen Sie nach dem Upgrade von vRealize Automation ein Upgrade von vRealize Log Insight aus.

Verfahren

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von vRealize Log Insight durch. Informationen hierzu finden Sie unter *Aktualisieren von vRealize Log Insight* in der [VMware vRealize Log Insight-Dokumentation](#).

Upgrade von einer in vRealize Automation integrierten vRealize Business for Cloud -Instanz

Wenn Sie Ihre vRealize Automation-Umgebung aktualisieren, müssen Sie die Registrierung Ihrer Verbindung zu vRealize Business for Cloud aufheben und erneut registrieren.

Führen Sie diesen Vorgang aus, um die Kontinuität des vRealize Business for Cloud-Diensts beim Upgrade Ihrer vRealize Automation-Umgebung sicherzustellen.

Verfahren

- 1 Aufheben der Registrierung von vRealize Business for Cloud für vRealize Automation. Weitere Informationen finden Sie unter *Aufheben der Registrierung von vRealize Business for Cloud für vRealize Automation* in der [VMware vRealize Business for Cloud-Dokumentation](#).
- 2 Führen Sie ein Upgrade von vRealize Automation durch.
- 3 Falls erforderlich, aktualisieren Sie vRealize Business for Cloud. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Business for Cloud* in der [VMware vRealize Business for Cloud-Dokumentation](#).
- 4 Registrieren Sie vRealize Business for Cloud bei vRealize Automation. Weitere Informationen finden Sie unter *Registrieren von vRealize Business for Cloud bei vRealize Automation* in der [VMware vRealize Business for Cloud-Dokumentation](#).

Vorbereiten des vRealize Automation -Upgrades

Führen Sie diese Aufgaben vor dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 durch.

Führen Sie diese Aufgaben in der Reihenfolge durch, in der sie in der Checkliste aufgeführt sind. Siehe [Checkliste für das Upgrade von vRealize Automation](#).

Durchführen der Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste vor dem vRealize Automation -Upgrade

Vor dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 müssen Sie eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in Ihrer vRealize Automation 7.1-, 7.2- oder 7.3-Umgebung durchführen.

Diese Datenerfassung ist erforderlich, damit die Neukonfiguration des Lastausgleichs in vRealize Automation 7.4 für 7.1-, 7.2- oder 7.3.x-Bereitstellungen möglich ist.

Verfahren

- ◆ Führen Sie eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in Ihrer vRealize Automation 7.1-, 7.2- oder 7.3.x-Umgebung vor dem Upgrade auf 7.4 durch. Weitere Informationen finden Sie unter [Manuelles Starten der Endpoint-Datenerfassung](#).

Nächste Schritte

[Sicherungsvoraussetzungen für das Upgrade von vRealize Automation 7.1, 7.2 oder 7.3 auf 7.4.](#)

Sicherungsvoraussetzungen für das Upgrade von vRealize Automation 7.1, 7.2 oder 7.3 auf 7.4

Erfüllen Sie die Sicherungsvoraussetzungen, bevor Sie mit dem Upgrade beginnen.

Voraussetzungen

- Überprüfen Sie, ob die Quellumgebung vollständig installiert und konfiguriert wurde.
- Melden Sie sich bei Ihrem vSphere Client an und sichern Sie für jede Appliance alle Konfigurationsdateien der vRealize Automation-Appliance in folgenden Verzeichnissen:
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Sichern Sie die IaaS Microsoft SQL Server-Datenbank. Suchen Sie im [Microsoft Developer Network](#) Artikel zur Erstellung einer vollständigen SQL Server-Datenbanksicherung, um weitere Informationen zu erhalten.
- Sichern Sie alle von Ihnen angepassten Dateien, wie zum Beispiel `DataCenterLocations.xml`.
- Erstellen Sie einen Snapshot aller virtuellen Appliances und IaaS-Server. Halten Sie die üblichen Richtlinien für das Sichern des gesamten Systems ein, falls das Upgrade von vRealize Automation fehlschlägt. Siehe [Sicherung und Wiederherstellung für vRealize Automation-Installationen](#).

Sichern Ihrer vorhandenen vRealize Automation -Umgebung

Fahren Sie vor dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 jeden vRealize Automation-iaaS-Server auf jedem Windows-Knoten und jede vRealize Automation-Appliance auf jedem Linux-Knoten herunter und erstellen Sie jeweils einen Snapshot. Wenn das Upgrade fehlschlägt, kehren Sie über den Snapshot zur letzten bekannten fehlerfreien Konfiguration zurück und versuchen Sie ein erneutes Upgrade.

Informationen zum Starten von vRealize Automation finden Sie unter [Starten von vRealize Automation](#).

Voraussetzungen

- [Sicherungsvoraussetzungen für das Upgrade von vRealize Automation 7.1, 7.2 oder 7.3 auf 7.4](#).
- Ab vRealize Automation 7.0 wird die PostgreSQL-Datenbank immer im Hochverfügbarkeitsmodus konfiguriert. Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance an und wählen Sie **vRA-Einstellungen > Datenbank** aus, um den aktuellen Master-Knoten zu suchen. Wenn die Datenbankkonfiguration als externe Datenbank aufgeführt ist, erstellen Sie eine manuelle Sicherung dieser externen Datenbank.
- Wenn die vRealize Automation Microsoft SQL-Datenbank nicht auf dem IaaS-Server gehostet wird, erstellen Sie eine Datenbanksicherungsdatei.
- Überprüfen Sie, ob die Sicherungsvoraussetzungen für das Upgrade erfüllt sind.
- Überprüfen Sie, ob ein Snapshot des Systems erstellt wurde, während es heruntergefahren war. Die ist die empfohlene Methode, einen Snapshot zu erstellen. Informationen hierzu finden Sie in der *vSphere 6.0-Dokumentation*.

Hinweis Wenn Sie die vRealize Automation-Appliance und die IaaS-Komponenten sichern, deaktivieren Sie speicherinterne und stillgelegte Snapshots.

- Wenn Sie die Datei `app.config` geändert haben, erstellen Sie eine Sicherung dieser Datei. Siehe [Wiederherstellung von vorgenommenen Änderungen an der Protokollierung in der app.config-Datei](#).
- Erstellen Sie eine Sicherung der externen Workflow-Konfigurationsdateien (xmldb). Siehe [Wiederherstellen von Dateien für die Zeitüberschreitung bei externen Workflows](#).
- Stellen Sie sicher, dass Sie über einen Speicherort außerhalb des aktuellen Ordners verfügen, an dem Sie die Sicherungsdatei speichern können. Siehe [Sicherungskopien von XML-Dateien führen zu einer Zeitüberschreitung des Systems](#).

Verfahren

- 1 Melden Sie sich bei Ihrem vSphere-Client an.
- 2 Suchen Sie jede vRealize Automation-iaaS-Windows-Maschine und jeden vRealize Automation-Appliance-Knoten.
- 3 Klicken Sie auf jeder Maschine auf **Gast herunterfahren** in der folgenden Reihenfolge.
 - a IaaS-Windows-Server-Maschinen
 - b vRealize Automation-Appliance.

- 4 Erstellen Sie einen Snapshot für jede vRealize Automation-Maschine.
- 5 Verwenden Sie Ihre bevorzugte Sicherungsmethode, um eine vollständige Sicherung jedes Appliance-Knotens zu erstellen.
- 6 Schalten Sie das System ein. Weitere Informationen finden Sie unter „Starten von vRealize Automation“ in *Verwalten von vRealize Automation*.

Führen Sie in einer Hochverfügbarkeitsumgebung diese Schritte durch, um Ihre virtuellen Appliances einzuschalten.

- a Starten Sie die vRealize Automation-Master-Appliance.
- b Melden Sie sich bei der Verwaltung der vRealize Automation-Appliance an, klicken Sie auf **Dienste** und warten Sie, bis der Lizenzierung-Dienststatus REGISTRIERT ist.
- c Starten Sie zur gleichen Zeit die verbleibenden vRealize Automation-Appliances.
- d Starten Sie den primären Webknoten und warten Sie, bis der Startvorgang abgeschlossen ist.
- e Starten Sie die primäre Manager Service-Maschine und warten Sie 2 bis 5 Minuten.

Die tatsächliche Zeit hängt von der Site-Konfiguration ab.

Hinweis 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.

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

Hinweis Sie können diese Komponenten in beliebiger Reihenfolge starten. Sie müssen nicht warten, bis eine Komponente abgeschlossen ist, bevor Sie eine andere starten.

- 7 Melden Sie sich bei jeder Verwaltungskonsole der vRealize Automation-Appliance an und vergewissern Sie sich, dass das System voll funktionsfähig ist.
 - a Klicken Sie auf **Dienste**.
 - b Stellen Sie sicher, dass jeder Dienst REGISTRIERT ist.

Nächste Schritte

[Festlegen des vRealize Automation PostgreSQL-Replikatmodus auf „asynchron“](#).

Festlegen des vRealize Automation PostgreSQL-Replikatmodus auf „asynchron“

Wenn Sie ein Upgrade von einer verteilten vRealize Automation-Umgebung aus durchführen, die im synchronen PostgreSQL-Replikatmodus arbeitet, müssen Sie vor dem Upgrade in einen asynchronen Modus wechseln.

Voraussetzungen

- Sie haben eine verteilte vRealize Automation-Umgebung, die Sie aktualisieren möchten.

- Sie sind als **Root-Benutzer** bei der Verwaltungsschnittstelle der vRealize Automation-Appliance (<https://vra-va-hostname.domain.name:5480>) angemeldet.

Verfahren

- 1 Klicken Sie auf **vRA-Einstellungen > Datenbank**.
- 2 Klicken Sie auf **Async-Modus** und warten Sie, bis die Aktion abgeschlossen ist.
- 3 Stellen Sie sicher, dass alle Knoten in der Spalte „Synchronisierungsstatus“ den Status Asynchron anzeigen.

Nächste Schritte

[Herunterladen von Updates für vRealize Automation-Appliances](#)

Herunterladen von Updates für vRealize Automation -Appliances

In der Verwaltungskonsolle Ihrer Appliance können Sie nach Updates suchen und die Updates mit einer der folgenden Methoden herunterladen.

Die beste Leistung lässt sich bei Upgrades mit der ISO-Dateimethode erzielen.

Um mögliche Probleme bei der Aktualisierung Ihrer Appliance oder bei Problemen während der Aktualisierung der Appliance zu vermeiden, lesen Sie den [VMware-Knowledgebase-Artikel vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database \(54987\)](#) (vRealize Automation-Upgrade schlägt aufgrund von Duplikaten in der vRealize Orchestrator-Datenbank fehl).

Herunterladen von Updates für virtuelle Appliances zur Verwendung mit einem CD-ROM-Laufwerk

Sie können Ihre virtuelle Appliance von einer ISO-Datei aktualisieren, die die Appliance vom virtuellen CD-ROM-Laufwerk liest. Dies ist die bevorzugte Methode.

Sie laden die ISO-Datei herunter und legen die primäre Appliance fest, um diese Datei zum Upgrade Ihrer Appliance zu verwenden.

Voraussetzungen

- Sichern Sie Ihre vorhandene vRealize Automation-Umgebung.
- Vergewissern Sie sich, dass alle in Ihrem Upgrade verwendeten CD-ROM-Laufwerke aktiviert sind, bevor Sie eine vRealize Automation-Appliance aktualisieren. Weitere Informationen zum Hinzufügen eines CD-ROM-Laufwerks zu einer virtuellen Maschine im vSphere-Client finden Sie in der vSphere-Dokumentation.

Verfahren

- 1 Laden Sie die ISO-Datei für das Update-Repository herunter.
 - a Starten Sie einen Browser und navigieren Sie zur [vRealize Automation-Produktseite](#) auf www.vmware.com.
 - b Klicken Sie auf **vRealize Automation-Downloads**, um zur Downloadseite von VMware zu gelangen.
 - c Laden Sie die entsprechende Datei herunter.
- 2 Suchen Sie die heruntergeladene Datei auf Ihrem System, um sicherzustellen, dass die Dateigröße der Größe der Datei auf der Downloadseite von VMware entspricht. Überprüfen Sie die Integrität Ihrer heruntergeladenen Datei mithilfe des Prüfsummenwerts, der auf der Downloadseite angegeben ist. Weitere Informationen finden Sie unter den Links unten auf der Downloadseite von VMware.
- 3 Vergewissern Sie sich, dass die primäre virtuelle Appliance eingeschaltet ist.
- 4 Verbinden Sie das CD-ROM-Laufwerk für die primäre virtuelle Appliance mit der ISO-Datei, die Sie heruntergeladen haben.
- 5 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 6 Klicken Sie auf die Registerkarte **Update**.
- 7 Klicken Sie auf **Einstellungen**.
- 8 Wählen Sie unter „Update-Repository“ die Option **CD-ROM-Updates verwenden** aus.
- 9 Klicken Sie auf **Einstellungen speichern**.

Herunterladen von Updates für vRealize Automation -Appliances aus einem VMware -Repository

Sie können das Update für Ihre vRealize Automation-Appliance aus einem öffentlichen Repository auf der vmware.com-Website herunterladen.

Voraussetzungen

- Sichern Sie Ihre vorhandene vRealize Automation-Umgebung.
- Stellen Sie sicher, dass die vRealize Automation-Appliance eingeschaltet ist.

Verfahren

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 2 Klicken Sie auf die Registerkarte **Update**.
- 3 Klicken Sie auf **Einstellungen**.

- 4 (Optional) Legen Sie im Bereich „Automatische Updates“ fest, wie oft nach Updates gesucht werden soll.
- 5 Wählen Sie im Bereich „Update-Repository“ die Option **Standard-Repository verwenden** aus.
Das Standard-Repository wird auf die korrekte VMware.com-URL festgelegt.
- 6 Klicken Sie auf **Einstellungen speichern**.

Aktualisierung der vRealize Automation -Appliance und der IaaS-Komponenten

Nachdem Sie die Upgrade-Voraussetzungen erfüllt und das Update der virtuellen Appliance heruntergeladen haben, installieren Sie das Update auf der vRealize Automation 7.1-, 7.2- oder 7.3.x-Appliance für die Aktualisierung auf 7.4.

In einer minimalen Umgebung installieren Sie das Update auf der vRealize Automation-Appliance. In einer verteilten Umgebung installieren Sie das Update auf dem Master-Appliance-Knoten. Die benötigte Zeit für das Abschließen des Updates hängt von Ihrer Umgebung und Ihrem Netzwerk ab. Wenn das Update abgeschlossen ist, zeigt das System die Änderungen auf der Seite „Update-Status“ der Verwaltungskonsole der vRealize Automation-Appliance an. Wenn das Update der Appliance abgeschlossen ist, müssen Sie die Appliance neu starten. Wenn Sie die Master-Appliance in einer verteilten Umgebung neu starten, startet das System jeden Replikatknoten neu.

Nach dem Neustart wird auf der Seite „Update-Status“ Folgendes angezeigt: Es wird darauf gewartet, dass VA-Dienste gestartet werden. Das IaaS-Update wird gestartet, wenn das System vollständig initialisiert ist und alle Dienste ausgeführt werden. Sie können den Fortschritt des IaaS-Upgrades auf der Seite „Update-Status“ verfolgen. Die Aktualisierung der ersten IaaS-Serverkomponente kann etwa 30 Minuten dauern. Während des Upgrades wird eine Meldung ähnlich der folgenden angezeigt: Serverkomponenten für Knoten web1-vra.mycompany.com werden aktualisiert.

Am Ende des Upgrade-Vorgangs für jeden Manager Service-Knoten wird eine Meldung ähnlich der folgenden angezeigt: Das automatische Manager Service-Failover wird auf folgendem Knoten aktiviert: node mgr-vra.mycompany.com. Ab vRealize Automation 7.3 kann die Auswahl, welcher Manager Service-Knoten zum Failover-Server wird, nicht mehr manuell getroffen werden, sondern wird vom System festgelegt. Diese Funktion wird während des Upgrades vom System aktiviert. Wenn Sie Probleme mit dieser Funktion haben, finden Sie weitere Informationen unter [Beim Update wird kein Upgrade des Management Agents durchgeführt](#).

Installieren des Updates auf der vRealize Automation -Appliance und den IaaS-Komponenten

Sie installieren das Update auf der virtuellen vRealize Automation 7.1-, 7.2- oder 7.3.x-Appliance, um ein Upgrade von vRealize Automation und den IaaS-Komponenten auf 7.4 durchzuführen.

Die Verwaltungskonsole dürfen Sie nicht schließen, während Sie das Update installieren.

Wenn beim Upgrade-Vorgang Probleme auftreten, erhalten Sie im Abschnitt [Fehlerbehebung bei vRealize Automation-Upgrades](#) Unterstützung.

Hinweis Beim Upgrade des Management-Agents auf den virtuellen IaaS-Maschinen wird ein öffentliches VMware-Zertifikat temporär in Ihrem Zertifikatspeicher für vertrauenswürdige Herausgeber installiert. Für das Upgrade des Management-Agents wird ein mit diesem Zertifikat signiertes PowerShell-Skript verwendet. Nach Abschluss des Upgrades wird dieses Zertifikat aus Ihrem Zertifikatspeicher entfernt.

Voraussetzungen

- Stellen Sie sicher, dass Sie eine Downloadmethode ausgewählt und das Verfahren für die Methode abgeschlossen haben. Siehe [Herunterladen von Updates für vRealize Automation-Appliances](#).
- Informationen zu allen Hochverfügbarkeitsumgebungen finden Sie unter [Sichern Ihrer vorhandenen vRealize Automation-Umgebung](#).
- Stellen Sie in Umgebungen mit Lastausgleichsdiensten sicher, dass Sie alle redundanten Knoten deaktiviert und die Integritätsüberwachungen entfernt haben. Weitere Informationen finden Sie in der Dokumentation Ihres Lastausgleichsdienstes.
 - vRealize Automation-Appliance
 - IaaS-Website
 - IaaS-Manager Service
- Vergewissern Sie sich, dass der Datenverkehr in Umgebungen mit Lastausgleichsdiensten nur an den primären Knoten geleitet wird.
- Überprüfen Sie mithilfe der folgenden Schritte, ob der in Microsoft Internetinformationsdienste (Internet Information Services, IIS) gehostete IaaS-Dienst ausgeführt wird:
 - a Starten Sie den Browser und geben Sie die URL **https://webhostname/Repository/Data/MetaModel.svc** ein, um zu überprüfen, ob das Web-Repository ausgeführt wird. Wenn die Überprüfung erfolgreich ist, werden keine Fehler zurückgegeben und eine Liste der Modelle wird im XML-Format angezeigt.
 - b Melden Sie sich bei der IaaS-Website an und vergewissern Sie sich, dass der Status in der `Repository.log`-Datei auf „OK“ gesetzt ist. Die Datei ist im VCAC-Basisordner unter `/Server/Model Manager Web/Logs/Repository.log` gespeichert.

Hinweis Melden Sie sich im Fall einer verteilten IaaS-Website bei der sekundären Website an (ohne MMD) und halten Sie Microsoft IIS vorübergehend an. Um sicherzustellen, dass der Datenverkehr des Lastausgleichsdienstes nur über den primären Webknoten geleitet wird, überprüfen Sie die `MetaModel.svc`-Konnektivität und starten Sie Microsoft IIS neu.

- Überprüfen Sie, ob sich alle IaaS-Knoten im fehlerfreien Zustand befinden, indem Sie die folgenden Schritte durchführen:
 - a Melden Sie sich auf der primären virtuellen Appliance bei der Verwaltung der vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.

- b Wählen Sie **vRA-Einstellungen > Cluster** aus.
- c Überprüfen Sie unter **Zuletzt verbunden** folgende Punkte.
 - Die IaaS-Knoten in der Tabelle weisen als Zeit der letzten Verbindung weniger als 30 Sekunden auf.
 - Die virtuellen Appliance-Knoten weisen als Zeit der letzten Verbindung weniger als 10 Minuten auf.

Wenn die IaaS-Knoten nicht mit der vRealize Automation-Appliance kommunizieren, schlägt das Upgrade fehl.

Um Konnektivitätsprobleme zwischen dem Management-Agent und der virtuellen Appliance zu untersuchen, führen Sie diese Schritte durch.

- 1 Melden Sie sich bei jedem IaaS-Knoten an, der nicht aufgeführt wird oder für den als Zeit für **Zuletzt verbunden** mehr als 30 Sekunden aufgeführt werden.
 - 2 Überprüfen Sie die Protokolle des Management-Agents, um festzustellen, ob Fehler aufgezeichnet wurden.
 - 3 Wenn der Management-Agent nicht ausgeführt wird, starten Sie den Agent in der Konsole „Dienste“ neu.
- d Beachten Sie in der Tabelle aufgeführte verwaiste Knoten. Ein verwaister Knoten ist ein doppelter Knoten, der auf dem Host gemeldet wird, aber auf dem Host nicht existiert. Sie müssen alle verwaisten Knoten löschen. Weitere Informationen finden Sie unter [Löschen von verwaisten Knoten in vRealize Automation](#).
- Falls Sie über eine virtuelle Replikat-Appliance verfügen, die nicht mehr Teil des Clusters ist, müssen Sie diese Appliance aus der Cluster-Tabelle löschen. Wenn Sie diese Appliance nicht entfernen, weist der Upgrade-Vorgang in einer Warnmeldung darauf hin, dass das Replikat-Update nicht erfolgreich war.
 - Vergewissern Sie sich, dass alle gespeicherten und laufenden Anforderungen erfolgreich abgeschlossen wurden, bevor Sie das Upgrade durchführen.
 - Wenn Sie die IaaS-Komponenten manuell aktualisieren, nachdem Sie die vRealize Automation 7.1-, 7.2- oder 7.3.x-Appliance aktualisiert haben, finden Sie weitere Informationen unter [Ausschließen des IaaS-Upgrades](#). Wenn Sie IaaS manuell aktualisieren möchten, müssen Sie alle IaaS-Dienste mit Ausnahme des Management-Agents auf jedem IaaS-Knoten beenden.

Verfahren

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.

Öffnen Sie in einer verteilten Umgebung die Verwaltungskonsole auf der Master-Appliance.
- 2 Klicken Sie auf **Dienste** und vergewissern Sie sich, dass alle Dienste registriert sind.

- 3 Wählen Sie **vRA-Einstellungen > Datenbank** aus und stellen Sie sicher, dass es sich um die Master-vRealize Automation-Appliance handelt.

Sie installieren das Update nur auf der Master-vRealize Automation-Appliance. Jede Replikat-vRealize Automation-Appliance wird mit der Master-Appliance aktualisiert.

- 4 Wählen Sie **Aktualisieren > Status** aus.
- 5 Klicken Sie auf **Nach Updates suchen**, um zu überprüfen, ob ein Update verfügbar ist.
- 6 (Optional) Klicken Sie für Instanzen der vRealize Automation-Appliance im Bereich „Appliance-Version“ auf **Details**, um Informationen zum Speicherort von Versionshinweisen anzuzeigen.
- 7 Klicken Sie auf **Updates installieren**.
- 8 Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die besagt, dass das Update ausgeführt wird. Das System zeigt die Änderungen, die während eines Upgrades vorgenommen werden, auf der Seite „Update-Zusammenfassung“ an. Die benötigte Zeit für das Abschließen des Updates hängt von Ihrer Umgebung und Ihrem Netzwerk ab.

- 9 (Optional) Um das Update detaillierter überwachen zu können, verwenden Sie einen Terminal-Emulator zur Anmeldung bei der primären Appliance. Zeigen Sie die Datei `updatecli.log` unter `/opt/vmware/var/log/vami/updatecli.log` an.

Die folgenden Dateien enthalten darüber hinaus weitere Informationen zum Upgrade-Fortschritt.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Wenn Sie sich während des Aktualisierungsvorgangs abmelden, können Sie den Update-Vorgang weiterhin in der Protokolldatei verfolgen. In der Datei `updatecli.log` werden möglicherweise Informationen zu der Version von vRealize Automation angezeigt, für die Sie das Upgrade durchführen. Diese angezeigte Version wird später im Upgrade-Vorgang in die entsprechende Version geändert.

- 10 Wenn das Update der vRealize Automation-Appliance abgeschlossen ist, klicken Sie in der Verwaltungskonsole auf **System > Neu starten**.

In einer verteilten Umgebung werden alle erfolgreich aktualisierten Replikat-Appliance-Knoten neu gestartet, wenn Sie die Master-Appliance neu starten.

Das IaaS-Update startet, wenn das System initialisiert wurde und alle Dienste eingerichtet sind und ausgeführt werden. Klicken Sie auf **Update > Status**, um den Fortschritt des IaaS-Upgrades zu beobachten.

- 11 Wenn das IaaS-Update abgeschlossen ist, klicken Sie in der Appliance-Verwaltungskonsole auf **Cluster** und stellen Sie sicher, dass die Versionsnummer für alle IaaS-Knoten und -Komponenten die aktuelle Version ist.

- 12 Klicken Sie in der Appliance-Verwaltungskonsole auf **Telemetrie**. Lesen Sie den Hinweis über die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) und wählen Sie aus, ob Sie an dem Programm teilnehmen möchten.

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>.

Weitere Informationen zum Programm zur Verbesserung der Kundenzufriedenheit finden Sie unter [Anmelden beim bzw. Abmelden vom VMware Programm zur Verbesserung der Kundenzufriedenheit für vRealize Automation](#).

Nächste Schritte

Wenn Ihre Bereitstellung einen Lastausgleich verwendet, führen Sie diese Schritte durch.

- 1 Aktivieren Sie die vRealize Automation-Integritätsprüfungen für den Lastausgleichsdienst.
- 2 Aktivieren Sie den Datenverkehr des Lastausgleichsdiensts für alle vRealize Automation-Knoten erneut.

Für den Fall, dass das Upgrade der IaaS-Komponenten fehlschlägt, finden Sie weitere Informationen unter [Getrenntes Upgrade der IaaS-Serverkomponenten, wenn das Upgrade fehlschlägt](#).

Getrenntes Upgrade der IaaS-Serverkomponenten, wenn das Upgrade fehlschlägt

Wenn der automatische Aktualisierungsvorgang fehlschlägt, können Sie die IaaS-Komponenten separat aktualisieren.

Wenn die vRealize Automation-IaaS-Website und der Manager Service erfolgreich aktualisiert wurden, können Sie das IaaS-Upgrade-Shell-Skript erneut ausführen, ohne die vor dem Upgrade erstellten Snapshots zurückzusetzen. In manchen Fällen kann ein ausstehendes Neustartereignis, das während des Upgrades mehrerer auf derselben virtuellen Maschine installierten IaaS-Komponenten generiert wurde, zum Fehlschlagen des Upgrades führen. Versuchen Sie in diesem Fall, den IaaS-Knoten manuell neu zu starten und das Upgrade erneut auszuführen, um das Problem zu beheben. Wenn das Upgrade weiterhin fehlschlägt, wenden Sie sich an den VMware-Support oder versuchen Sie mit den folgenden Schritten, ein manuelles Upgrade durchzuführen.

- 1 Wiederherstellen der vRealize Automation-Appliance mit dem Zustand vor dem Upgrade.
- 2 Führen Sie einen Befehl zum Ausschließen der IaaS-Komponenten aus dem Aktualisierungsvorgang aus. Siehe [Ausschließen des IaaS-Upgrades](#).
- 3 Führen Sie den Aktualisierungsvorgang auf der vRealize Automation-Appliance aus.
- 4 Aktualisieren Sie die IaaS-Komponenten separat mithilfe des Upgrade-Shell-Skripts oder des MSI-Pakets des vRealize Automation 7.4-IaaS-Installationsprogramms.

Upgrade der IaaS-Komponenten unter Verwendung des Upgrade-Shell-Skripts nach dem Upgrade der vRealize Automation -Appliance

Aktualisieren Sie die IaaS-Komponenten mithilfe des Upgrade-Shell-Skripts, nachdem Sie das Update für alle vRealize Automation 7.1-, 7.2- oder 7.3.x-Appliances auf 7.4 durchgeführt haben.

Die aktualisierte vRealize Automation-Appliance enthält ein Shell-Skript, das Sie zum Upgrade jedes IaaS-Knotens und jeder Komponente verwenden.

Sie können das Upgrade-Skript ausführen, indem Sie die vSphere-Konsole für die virtuelle Maschine oder eine SSH-Konsolensitzung verwenden. Wenn Sie die vSphere-Konsole verwenden, vermeiden Sie temporäre Probleme bei der Netzwerkkonnektivität, die zur fehlerhaften Ausführung des Skripts führen können.

Wenn Sie das Skript während des Upgrades einer Komponente anhalten, wird das Skript nach dem Abschließen des Upgrades der Komponente beendet. Wenn noch andere Komponenten auf dem Knoten aktualisiert werden müssen, können Sie das Skript erneut ausführen.

Nach Abschluss des Upgrades können Sie das Upgrade-Ergebnis überprüfen, indem Sie die Upgrade-Protokolldatei im Verzeichnis `/opt/vmware/var/log/vami/upgrade-iaas.log` öffnen.

Voraussetzungen

- Lesen Sie [Fehlerbehebung bei vRealize Automation-Upgrades](#) durch.
- Vergewissern Sie sich, dass alle vRealize Automation-Appliances erfolgreich aktualisiert wurden.
- Wenn Sie einen IaaS-Server nach dem Aktualisieren aller vRealize Automation-Appliances und vor dem Upgrade der IaaS-Komponenten neu starten, beenden Sie alle IaaS-Dienste unter Windows mit Ausnahme des Management-Agent-Dienstes.
- Bevor Sie das Upgrade-Shell-Skript auf dem Masterknoten der vRealize Automation-Appliance ausführen, klicken Sie auf der Verwaltungskonsole der Appliance auf **Dienste**. Stellen Sie sicher, dass jeder Dienst außer dem IaaS-Dienst registriert ist.
- Um den IaaS-Management-Agent manuell auf jedem IaaS-Knoten zu installieren, führen Sie die folgenden Schritte durch.
 - a Öffnen Sie einen Browser und wechseln Sie zur Seite „VMware vRealize Automation-IaaS-Installation“ auf der Appliance unter `https://virtual_appliance_host_FQDN:5480/installer`.
 - b Laden Sie das Installationsprogramm für den Management-Agent, `vCAC-IaaSManagement-Agent-Setup.msi`, herunter.
 - c Melden Sie sich bei jeder vRealize Automation-IaaS-Maschine an und führen Sie das Upgrade des Management-Agent mit dem Installationsprogramm des Management-Agents durch. Starten Sie den Windows-Management-Agent-Dienst neu.
- Stellen Sie sicher, dass die primäre IaaS-Website und der Model Manager-Knoten über JAVA SE Runtime Environment 8, 64 Bit, Update 161 oder höher verfügen. Nach der Installation von Java müssen Sie die Umgebungsvariable, `JAVA_HOME`, auf jedem Serverknoten auf die neue Version festlegen.

- Melden Sie sich bei jedem IaaS-Websiteknoten an und stellen Sie sicher, dass das Erstellungsdatum für die Datei `web.config` vor dem Änderungsdatum liegt. Wenn das Erstellungsdatum für die Datei `web.config` mit dem Änderungsdatum übereinstimmt oder dahinter liegt, führen Sie den Vorgang in [Upgrade für die IaaS-Website-Komponente schlägt fehl](#) aus.
- Um sicherzustellen, dass jeder IaaS-Knoten über einen aktualisierten IaaS-Management-Agent verfügt, führen Sie diese Schritte auf jedem IaaS-Knoten durch:
 - a Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance an.
 - b Wählen Sie **vRA-Einstellungen > Cluster** aus.
 - c Erweitern Sie die Liste aller installierten Komponenten für jeden IaaS-Knoten und suchen Sie den IaaS-Management-Agent.
 - d Stellen Sie sicher, dass der Management-Agent auf die aktuelle Version aktualisiert wurde.
- [Ausschließen des IaaS-Upgrades](#).
- Vergewissern Sie sich, dass Sie auf die IaaS-Microsoft SQL Server-Datenbank zugreifen können, falls Sie ein Rollback durchführen müssen.
- Vergewissern Sie sich, dass Snapshots der IaaS-Server in Ihrer Bereitstellung verfügbar sind.

Wenn das Upgrade nicht erfolgreich ist, stellen Sie den Snapshot und das Datenbank-Update wieder her und versuchen Sie es erneut.

Verfahren

- 1 Öffnen Sie eine neue Konsolensitzung auf dem vRealize Automation-Appliance-Host. Melden Sie sich mit dem Root-Konto an.
- 2 Wechseln Sie zum Verzeichnis `/usr/lib/vcac/tools/upgrade/`.

Es ist wichtig, dass alle IaaS-Management-Agents vor der Ausführung des `./upgrade-Shell-Skripts` ordnungsgemäß aktualisiert wurden. Wenn ein IaaS-Management-Agent während des Ausführens des Shell-Skripts ein Problem aufweist, siehe [Beim Update wird kein Upgrade des Management Agents durchgeführt](#).
- 3 Führen Sie das Upgrade-Skript aus.
 - a Geben Sie in der Eingabeaufforderung `./upgrade` ein.
 - b Drücken Sie die Eingabetaste.

Eine Beschreibung des IaaS-Upgrade-Vorgangs finden Sie unter [Aktualisierung der vRealize Automation-Appliance und der IaaS-Komponenten](#).

Wenn das Upgrade-Shell-Skript fehlschlägt, sehen Sie sich die Datei `upgrade-iaas.log` an.

Sie können das Upgrade-Skript erneut ausführen, nachdem Sie das Problem behoben haben.

Nächste Schritte

- 1 [Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator-Control Center](#).

- 2 Wenn in Ihrer Bereitstellung ein Lastausgleichsdienst verwendet wird, aktivieren Sie die vRealize Automation-Integritätsüberwachungen und den Datenverkehr zu allen Knoten erneut.

Weitere Informationen finden Sie unter *vRealize Automation-Lastausgleich*.

Upgrade von IaaS-Komponenten mithilfe der ausführbaren Datei des IaaS-Installationsprogramms nach dem Upgrade der vRealize Automation -Appliance

Sie können diese alternative Methode für das Upgrade der IaaS-Komponenten nach dem Upgrade der vRealize Automation 7.1-, 7.2- oder 7.3.x-Appliance auf 7.4 verwenden.

Herunterladen des IaaS-Installationsprogramms zum Upgrade von IaaS-Komponenten nach dem Upgrade der vRealize Automation -Appliance

Laden Sie nach dem Upgrade der vRealize Automation-Appliance auf 7.4 das IaaS-Installationsprogramm auf die Maschine herunter, auf der die IaaS-Komponenten für das Upgrade installiert sind.

Etwasige Zertifikatswarnungen während dieses Vorgangs können ignoriert werden.

Hinweis Außer für eine passive Sicherungsinstanz des Manager Service muss der Starttyp für alle Dienste während des Upgrades auf „Automatisch“ eingestellt sein. Das Upgrade schlägt fehl, wenn Sie die Dienste auf „Manuell“ einstellen.

Voraussetzungen

- Stellen Sie sicher, dass Microsoft .NET Framework 4.5.2 oder höher auf der IaaS-Installationsmaschine installiert ist. Das .NET-Installationsprogramm können Sie von der Webseite für das vRealize Automation-Installationsprogramm herunterladen. Wenn Sie .NET auf Version 4.5.2 aktualisieren, nachdem Sie die Dienste heruntergefahren haben und die Maschine im Rahmen der Installation neu gestartet wurde, müssen Sie alle IaaS-Dienste außer dem Management-Agent manuell beenden.
- Achten Sie bei Verwendung von Internet Explorer zum Herunterladen darauf, dass „Verstärkte Sicherheitskonfiguration“ nicht aktiviert ist. Geben Sie `res://iesetup.dll/SoftAdmin.htm` in die Suchleiste ein und drücken Sie die Eingabetaste.
- Melden Sie sich als Administrator bei dem Windows-Server an, auf dem eine oder mehrere der zu aktualisierenden IaaS-Komponenten installiert sind.

Verfahren

- 1 Starten Sie einen Webbrowser.
- 2 Geben Sie die URL für die Downloadseite des Windows-Installationsprogramms ein.
Beispiel: `https://vcac-va-hostname.domain.name:5480/installer`, wobei `vcac-va-hostname.domain.name` der Name des primären vRealize Automation-Appliance-Knotens (Master) ist.
- 3 Klicken Sie auf den Link **IaaS-Installationsprogramm**.

- Speichern Sie, wenn Sie dazu aufgefordert werden, die Installationsdatei, „setup__vcac-va-hostname.domain.name@5480.exe“, auf dem Desktop.

Ändern Sie den Dateinamen nicht. Er wird verwendet, um die Installation mit der vRealize Automation-Appliance zu verbinden.

Nächste Schritte

[Upgrade der IaaS-Komponenten nach dem Upgrade von vRealize Automation 7.1 oder 7.2 auf 7.3.](#)

Upgrade der IaaS-Komponenten nach dem Upgrade von vRealize Automation 7.1 oder 7.2 auf 7.3

Sie müssen die SQL-Datenbank aktualisieren und alle Systeme konfigurieren, auf denen IaaS-Komponenten installiert sind. Sie können diese Schritte für Minimal- und verteilte Installationen befolgen.

Hinweis Das IaaS-Installationsprogramm muss sich auf der Maschine befinden, die die IaaS-Komponenten enthält, für die Sie ein Upgrade durchführen möchten. Sie können das Installationsprogramm nicht von einem externen Standort ausführen, mit Ausnahme der Microsoft SQL-Datenbank, die auch aus der Ferne über den Webknoten aktualisiert werden kann.

Vergewissern Sie sich, dass Snapshots der IaaS-Servers in Ihrer Bereitstellung verfügbar sind. Wenn die Aktualisierung fehlschlägt, können Sie den Snapshot wiederherstellen und eine erneute Aktualisierung versuchen.

Führen Sie die Aktualisierung so durch, dass die Dienste in folgender Reihenfolge aktualisiert werden:

- IaaS-Websites

Wenn Sie einen Lastausgleichsdienst verwenden, deaktivieren Sie den Datenverkehr auf allen nicht primären Knoten.

Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren, der einen Website-Dienst ausführt. Starten Sie mit dem Server, auf dem die Komponente „Model Manager-Daten“ installiert ist.

Wenn Sie ein manuelles Upgrade der externen Microsoft SQL-Datenbank durchführen, müssen Sie vor der Aktualisierung des Webknotens die externe SQL-Datenbank aktualisieren. Sie können ein Upgrade der externen SQL aus der Ferne über den Webknoten durchführen.

- Manager Services

Führen Sie zunächst ein Upgrade des aktiven Manager Services und dann des passiven Manager Services durch.

Falls die SSL-Verschlüsselung in Ihrer SQL-Instanz nicht aktiviert ist, deaktivieren Sie das Kontrollkästchen für die SSL-Verschlüsselung im Konfigurationsdialogfeld für die IaaS-Aktualisierung neben der SQL-Definition.

- DEM-Orchestrator und -Workers

Aktualisieren Sie alle DEM-Orchestratoren und -Workers. Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren.

4 Agents

Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren, der einen Agent ausführt.

5 Management-Agent

Wird im Rahmen des Aktualisierungsprozesses automatisch aktualisiert.

Wenn Sie verschiedene Dienste auf einem Server verwenden, werden bei der Aktualisierung die Dienste in der richtigen Reihenfolge aktualisiert. Wenn Ihre Site z. B. Website-Dienste und Manager Services auf dem gleichen Server hat, wählen Sie beide für die Aktualisierung aus. Das Aktualisierungs-Installationsprogramm wendet die Updates in der richtigen Reihenfolge an. Sie müssen die Aktualisierung auf einem Server abschließen, bevor Sie mit der Aktualisierung eines anderen Servers beginnen.

Hinweis Wenn Ihre Bereitstellung einen Lastausgleichsdienst verwendet, muss die primäre Appliance mit dem Lastausgleichsdienst verbunden sein. Alle anderen Instanzen von vRealize Automation-Appliance-Appliances müssen für den Datenverkehr des Lastausgleichsdiensts deaktiviert werden, bevor Sie die Aktualisierung anwenden, um Cachefehler zu vermeiden.

Voraussetzungen

- Sichern Sie Ihre bestehende vRealize Automation-Umgebung.
- Wenn Sie einen IaaS-Server nach dem Aktualisieren aller vRealize Automation-Appliances und vor dem Upgrade der IaaS-Komponenten neu starten, beenden Sie alle IaaS-Windows-Dienste mit Ausnahme des Management-Agent-Diensts auf dem Server.
- [Herunterladen des IaaS-Installationsprogramms zum Upgrade von IaaS-Komponenten nach dem Upgrade der vRealize Automation-Appliance.](#)
- Stellen Sie sicher, dass die primäre IaaS-Website, die Microsoft SQL-Datenbank und der Model Manager-Knoten über JAVA SE Runtime Environment 8, 64 Bit, Update 111 oder höher verfügen. Nach der Installation von Java müssen Sie die Umgebungsvariable, JAVA_HOME, auf jedem Serverknoten auf die neue Version festlegen.
- Stellen Sie sicher, dass das Datum der Dateierstellung in der Datei `web.config` vor dem Änderungsdatum liegt. Wenn das Erstellungsdatum für die Datei `web.config` mit dem Änderungsdatum übereinstimmt oder dahinter liegt, führen Sie den Vorgang in [Upgrade für die IaaS-Website-Komponente schlägt fehl](#) aus.
- Führen Sie diese Schritte durch, um den Microsoft Distributed Transaction Coordinator (DTC) neu zu konfigurieren.

Hinweis Selbst wenn der Distributed Transaction Coordinator aktiviert ist, kann die verteilte Transaktion fehlschlagen, wenn die Firewall aktiviert ist.

- a Wählen Sie in der vRealize Automation-Appliance **Start > Verwaltung > Komponentendienste** aus.

- b Erweitern Sie **Komponentendienste > Computer > Mein Computer > Distributed Transaction Coordinator**.
- c Wählen Sie die entsprechende Aufgabe aus.
 - Bei einem eigenständigen lokalen DTC klicken Sie mit der rechten Maustaste auf **Lokaler DTC** und wählen Sie **Eigenschaften** aus.
 - Bei einem Cluster-DTC erweitern Sie **Cluster-DTCs**, klicken Sie mit der rechten Maustaste auf den benannten Cluster-DTC und wählen Sie **Eigenschaften** aus.
- d Klicken Sie auf **Sicherheit**.
- e Wählen Sie alle folgenden Optionen aus:
 - **DTC-Netzwerkzugriff**
 - **Remote-Clients zulassen**
 - **Eingehende zulassen**
 - **Ausgehende zulassen**
 - **Gegenseitige Authentifizierung erforderlich**
- f Klicken Sie auf **OK**.

Verfahren

- 1 Wenn Sie einen Lastausgleichsdienst verwenden, bereiten Sie die Umgebung vor.
 - a Stellen Sie sicher, dass der IaaS-Websiteknoten, der die Model Manager-Daten enthält, für den Datenverkehr des Lastausgleichsdiensts aktiviert ist.

Diesen Knoten erkennen Sie am Vorhandensein des Ordners `VCAC-Ordner\Server\Config-Tool`.
 - b Deaktivieren Sie alle anderen IaaS-Websites und nicht-primären Manager Services für den Datenverkehr des Lastausgleichsdiensts.
- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 3 Klicken Sie auf **Weiter**.
- 4 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 5 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für Ihre aktuelle Bereitstellung ein.

Der Benutzername lautet **root** und das Kennwort ist dasjenige, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 6 Wählen Sie **Zertifikat akzeptieren** aus.
- 7 Vergewissern Sie sich auf der Seite **Installationstyp**, dass **Aktualisierung** ausgewählt ist.

Wenn **Aktualisierung** nicht ausgewählt ist, sind die Komponenten auf diesem System bereits auf diese Version aktualisiert.

- 8 Klicken Sie auf **Weiter**.
- 9 Konfigurieren Sie die Aktualisierungseinstellungen.

Option	Aktion
Beim Aktualisieren der Model Manager-Daten	<p>Aktivieren Sie das Kontrollkästchen Model Manager-Daten im Abschnitt „vCAC-Server“.</p> <p>Das Kontrollkästchen ist standardmäßig aktiviert. Aktualisieren Sie Model Manager-Daten nur einmal. Wenn Sie die Setup-Datei auf mehreren Maschinen ausführen, um eine verteilte Installation zu aktualisieren, funktionieren die Webserver nicht mehr, während die Versionen der Webserver und der Model Manager-Daten nicht übereinstimmen. Wenn Sie die Model Manager-Daten und alle Webserver aktualisiert haben, sollten alle Webserver funktionieren.</p>
Keine Aktualisierung der Model Manager-Daten	<p>Deaktivieren Sie das Kontrollkästchen Model Manager-Daten im Abschnitt „vCAC-Server“.</p>
So behalten Sie angepasste Workflows als neueste Version in den Model Manager-Daten bei	<p>Wenn Sie die Model Manager-Daten aktualisieren, aktivieren Sie das Kontrollkästchen Meine neuesten Workflow-Versionen beibehalten im Abschnitt der Erweiterbarkeits-Workflows.</p> <p>Das Kontrollkästchen ist standardmäßig aktiviert. Angepasste Workflows werden immer beibehalten. Mit dem Kontrollkästchen wird nur die Reihenfolge der Versionen bestimmt. Wenn Sie vRealize Automation Designer zum Benutzerdefinieren von Workflows im Model Manager verwendet haben, wählen Sie diese Option, um die neueste Version jedes benutzerdefinierten Workflows vor der Aktualisierung als neueste Version nach der Aktualisierung beizubehalten.</p> <p>Wenn Sie diese Option nicht auswählen, wird die mit vRealize Automation Designer bereitgestellte Version jedes Workflows die neueste Version nach der Aktualisierung, und die neueste Version vor der Aktualisierung wird zur zweitneuesten.</p> <p>Informationen zu vRealize Automation Designer finden Sie in Erweitern des Maschinenlebenszyklus mithilfe von vRealize Automation Designer.</p>
Beim Upgrade eines Distributed Execution Manager oder eines Proxy-Agents	<p>Geben Sie die Anmeldedaten für das Administratorkonto im Abschnitt des Dienstkontos ein.</p> <p>Alle Dienste, die Sie aktualisieren, werden unter diesem Konto ausgeführt.</p>
So geben Sie die Microsoft SQL Server-Datenbank an	<p>Wenn Sie die Model Manager-Daten aktualisieren, geben Sie die Namen des Datenbankservers und der Datenbankinstanz in das Textfeld Server im Abschnitt der Installationsinformationen für die Microsoft SQL Server-Datenbank ein. Geben Sie einen vollqualifizierten Domännennamen (FQDN) als Datenbankservernamen in das Textfeld Datenbankname ein.</p> <p>Wenn die Datenbank sich an einem anderen als dem Standard-SQL-Port befindet, geben Sie in der Spezifikation der Serverinstanz die Portnummer an. Die Microsoft SQL-Standardportnummer lautet 1433.</p> <p>Beim Aktualisieren der Managerknoten wird die MSSQL-SSL-Option standardmäßig ausgewählt. Wenn Ihre Datenbank SSL nicht verwendet, deaktivieren Sie SSL für Datenbankverbindung verwenden.</p>

- 10 Klicken Sie auf **Weiter**.
- 11 Vergewissern Sie sich, dass alle zu aktualisierenden Dienste auf der Seite „Bereit für Upgrade“ aufgeführt werden, und klicken Sie auf **Aktualisieren**.

Die Aktualisierungsseite und eine Statusanzeige werden angezeigt. Nachdem der Aktualisierungsprozess abgeschlossen ist, wird die Schaltfläche **Weiter** aktiv.

- 12 Klicken Sie auf **Weiter**.
- 13 Klicken Sie auf **Beenden**.
- 14 Vergewissern Sie sich, dass alle Dienste neu gestartet wurden,
- 15 Wiederholen Sie diese Schritte für jeden IaaS-Server in Ihrer Bereitstellung in der empfohlenen Reihenfolge.
- 16 Nachdem alle Komponenten aktualisiert wurden, melden Sie sich bei der Verwaltungskonsole der Appliance an und vergewissern Sie sich, dass jetzt alle Dienste, darunter auch IaaS, registriert sind.
- 17 (Optional) Aktivieren Sie das automatische Manager Service-Failover. Siehe [Aktivieren des automatischen Manager Service-Failovers nach einem Upgrade](#).

Alle ausgewählten Komponenten werden auf die neue Version aktualisiert.

Nächste Schritte

- 1 [Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator-Control Center](#).
- 2 Wenn in Ihrer Bereitstellung ein Lastausgleichsdienst verwendet wird, aktualisieren Sie für jeden Lastausgleichsdienstknoten die Verwendung von vRealize Automation-Integritätsprüfungen und aktivieren Sie den Datenverkehr des Lastausgleichsdiensts wieder für alle nicht verbundenen Knoten.

Weitere Informationen finden Sie unter *vRealize Automation-Lastausgleich*.

Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator -Control Center

Nach dem Upgrade der IaaS-Serverkomponenten müssen Sie den Zugriff auf vRealize Orchestrator wiederherstellen.

Wenn Sie ein Upgrade von vRealize Automation 7.3 und früher auf 7.4 durchführen, müssen Sie wie folgt vorgehen, damit die neue Funktion „Rollenbasierte Zugriffssteuerung“ funktioniert. Dieses Verfahren ist für eine Hochverfügbarkeitsumgebung vorgesehen.

Voraussetzungen

Erstellen Sie einen Snapshot Ihrer vRealize Automation-Umgebung.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance-Verwaltungskonsole als Root-Benutzer an, indem Sie den vollqualifizierten Domännennamen des Appliance-Hosts, `https://va-hostname.domain.name:5480` verwenden.
- 2 Wählen Sie **vRA-Einstellungen > Datenbank** aus.
- 3 Identifizieren Sie den Master- und die Replikatknoten.
- 4 Öffnen Sie auf jedem Replikatknoten eine SSH-Sitzung, melden Sie sich als Administrator an und führen Sie den folgenden Befehl aus:

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

- 5 Öffnen Sie auf dem Masterknoten eine SSH-Sitzung, melden Sie sich als Administrator an und führen Sie den folgenden Befehl aus:

```
rm /etc/vco/app-server/vco-registration-id
```

- 6 Wechseln Sie auf dem Masterknoten zum Verzeichnis `/etc/vco/app-server/`.

- 7 Öffnen Sie die Datei `sso.properties`.

- 8 Wenn der Eigenschaftsname `com.vmware.o11n.sso.admin.group.name` Leerzeichen oder andere Bash-Zeichen enthält, die als Sonderzeichen in einem Bash-Befehl akzeptiert werden können, wie etwa einen Bindestrich (-) oder ein Dollarzeichen (\$), führen Sie die folgenden Schritte aus.

- a Kopieren Sie die Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name` und geben Sie als Wert `AdminGroup` ein.
- b Fügen Sie am Beginn der ursprünglichen Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name` ein Hash-Zeichen (#) hinzu, um die Zeile auszukommentieren.
- c Speichern und schließen Sie die Datei `sso.properties`.

- 9 Führen Sie den folgenden Befehl aus:

```
vcac-vami vco-service-reconfigure
```

- 10 Öffnen Sie die Datei `sso.properties`. Wenn die Datei geändert wurde, führen Sie die folgenden Schritte aus.

- a Entfernen Sie das Hash-Zeichen (#) vom Beginn der ursprünglichen Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name`, um die Auskommentierung der Zeile aufzuheben.
- b Entfernen Sie die Kopie der Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name`.
- c Speichern und schließen Sie die Datei `sso.properties`.

- 11 Führen Sie den folgenden Befehl aus, um den `vco-server`-Dienst neu zu starten:

```
service vco-server restart
```

- 12 Führen Sie den folgenden Befehl aus, um den `vco-configurator`-Dienst neu zu starten:

```
service vco-configurator restart
```

- 13 Klicken Sie in der vRealize Automation-Appliance-Verwaltungskonsole auf **Dienste** und warten Sie, bis alle Dienste auf dem Masterknoten REGISTRIERT sind.

- 14 Wenn alle Dienste registriert sind, fügen Sie die vRealize Automation-Replikatknoten dem vRealize Automation-Cluster hinzu, um die vRealize Orchestrator-Konfiguration zu synchronisieren. Weitere Informationen hierzu finden Sie unter [Neukonfigurieren des integrierten vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit](#).

Nächste Schritte

[Upgrade von vRealize Orchestrator nach dem Upgrade von vRealize Automation.](#)

Upgrade von vRealize Orchestrator nach dem Upgrade von vRealize Automation

Sie müssen Ihre vRealize Orchestrator-Instanz aktualisieren, wenn Sie ein Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 durchführen.

In vRealize Orchestrator 7.4 stehen Ihnen beim Upgrade auf vRealize Automation 7.4 zwei Optionen zur Aktualisierung von vRealize Orchestrator zur Verfügung.

- Sie können Ihren vorhandenen externen vRealize Orchestrator-Server auf die eingebettete vRealize Orchestrator-Instanz aktualisieren, die in vRealize Automation 7.4 enthalten ist.
- Sie können ein Upgrade Ihres vorhandenen eigenständigen oder geclusterten vRealize Orchestrator-Servers durchführen, sodass er mit vRealize Automation 7.4 funktioniert.

Migrieren eines externen vRealize Orchestrator -Servers zu vRealize Automation

Sie können Ihren vorhandenen externen vRealize Orchestrator-Server zu einer in vRealize Automation 7.4 eingebetteten vRealize Orchestrator-Instanz migrieren.

Sie können vRealize Orchestrator als externe Serverinstanz bereitstellen und vRealize Automation für die Verwendung mit dieser externen Instanz konfigurieren oder Sie können den vRealize Orchestrator-Server, der in der vRealize Automation-Appliance enthalten ist, konfigurieren und verwenden.

VMware empfiehlt, dass Sie Ihre externe vRealize Orchestrator-Instanz zu dem Orchestrator-Server migrieren, der in vRealize Automation integriert ist. Die Migration von einer externen zu einer eingebetteten Orchestrator-Instanz bietet folgende Vorteile:

- Reduzierung der Gesamtbetriebskosten
- Vereinfachung des Bereitstellungsmodells
- Verbesserung der betrieblichen Effizienz

Hinweis Ziehen Sie in Betracht, die externe vRealize Orchestrator-Instanz in den folgenden Fällen zu verwenden:

- Mehrere Mandanten in der vRealize Automation-Umgebung
- Geografisch verteilte Umgebung
- Bewältigung von Workloads
- Verwendung bestimmter Plugins, wie z. B. ältere Versionen des Site Recovery Manager-Plugins

Control Center-Unterschiede zwischen externer und eingebetteter Orchestrator-Instanz

Einige Menüoptionen, die im Control Center einer externen vRealize Orchestrator-Instanz verfügbar sind, sind nicht in der Standardansicht des Control Center einer eingebetteten Orchestrator-Instanz enthalten.

Einige Optionen sind im Control Center des eingebetteten Orchestrator-Servers standardmäßig ausgeblendet.

Menüoption	Details
Lizenzierung	Die eingebettete Orchestrator-Instanz ist so vorkonfiguriert, dass vRealize Automation als Lizenzgeber verwendet wird.
Konfiguration exportieren/ importieren	Die Konfiguration der eingebetteten Orchestrator-Instanz ist in den exportierten vRealize Automation-Komponenten enthalten.
Datenbank konfigurieren	Die eingebettete Orchestrator-Instanz verwendet die Datenbank, die von vRealize Automation genutzt wird.
Programm zur Verbesserung der Kundenzufriedenheit	Über die Schnittstelle zur Verwaltung der vRealize Automation-Appliance können Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen. Lesen Sie die Informationen unter <i>Programm zur Verbesserung der Benutzerfreundlichkeit</i> im Handbuch <i>Verwalten von vRealize Automation</i> .

Andere nicht in der Standardansicht des Control Centers sichtbare Optionen sind das Textfeld **Hostadresse** und die Schaltfläche **REGISTRIERUNG AUFHEBEN** auf der Seite **Anbieter für Authentifizierung konfigurieren**.

Hinweis Wenn Sie sich über die vollständige Gruppe der Control Center-Optionen in vRealize Orchestrator, die in vRealize Automation integriert ist, informieren möchten, müssen Sie unter https://vra-va-Hostname.Domäne.Name_oder_Lastausgleichsadresse:8283/vco-controlcenter/#/?advanced die Seite für die erweiterte Verwaltung von Orchestrator aufrufen und diese mit der Funktionstaste F5 auf der Tastatur aktualisieren.

Migrieren einer externen Instanz von vRealize Orchestrator 7.x auf vRealize Automation 7.4

Sie können die Konfiguration aus Ihrer bestehenden externen Orchestrator-Instanz exportieren und sie in den in vRealize Automation integrierten Orchestrator-Server importieren.

Hinweis Wenn Sie mehrere vRealize Automation-Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren oder migrieren Sie Ihre vRealize Automation-Instanz auf Version 7.4. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Automation* im Handbuch *Installieren oder Upgrade von vRealize Automation*.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Exportieren Sie die Konfiguration aus dem externen Orchestrator-Server.
 - a Melden Sie sich beim Control Center des externen Orchestrator-Servers als **root** oder als **Administrator** an (je nach Quellversion).
 - b Beenden Sie den Orchestrator-Serverdienst über die Seite **Startoptionen**, um unerwünschte Änderungen an der Datenbank zu vermeiden.
 - c Wechseln Sie zur Seite **Konfiguration exportieren/importieren**.
 - d Wählen Sie auf der Seite **Konfiguration exportieren** die Optionen **Serverkonfiguration exportieren**, **Paket-Plug-Ins** und **Plug-In-Konfigurationen exportieren**.

- 2 Migrieren Sie die exportierte Konfiguration in die eingebettete Orchestrator-Instanz.
 - a Laden Sie die exportierte Orchestrator-Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation-Appliance hoch.
 - b Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
 - c Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

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

- d Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
```

- 3 Wenn der externe Orchestrator-Server, von dem aus Sie migrieren möchten, die integrierte PostgreSQL-Datenbank verwendet, bearbeiten Sie deren Datenbankkonfigurationsdateien.
 - a Heben Sie in der Datei `/var/vmware/vpostgres/current/pgdata/postgresql.conf` die Kommentierung der Zeile `listen_addresses` auf.
 - b Legen Sie als Werte für `listen_addresses` Platzhalter (*) fest.

```
listen_addresses = '*'
```

- c Fügen Sie in der Datei `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` eine Zeile an.

```
host all all vra-va-ip-address/32 md5
```

Hinweis Die Datei `pg_hba.conf` erfordert die Verwendung eines CIDR-Präfixformats anstelle einer IP-Adresse und Subnetzmaske.

- d Starten Sie den PostgreSQL-Serverdienst neu.

```
service vpostgres restart
```

- 4 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

PostgreSQL: `jdbc:postgresql://Host:Port/Datenbankname`

MSSQL: `jdbc:jtds:sqlserver://Host:Port/Datenbankname\;` if using SQL authentication and MSSQL: `jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@Host:Port:Datenbankname`

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

- 5 Entfernen Sie alle Zertifikate aus dem Keystore der Datenbank.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Installieren Sie die Orchestrator-Plug-Ins erneut.
- Melden Sie sich beim Control Center als **root** an.
 - Klicken Sie auf **Fehlerbehebung**.
 - Klicken Sie auf **Plug-In-Neuinstallation erzwingen**.
- 7 Starten Sie den Orchestrator-Serverdienst.

- 8 Setzen Sie das System auf die Standardkonfiguration der Datei `postgresql.conf` und `pg_hba.conf` zurück.
 - a Starten Sie den PostgreSQL-Serverdienst neu.

Damit haben Sie erfolgreich eine externe Orchestrator-Serverinstanz zu einer vRealize Orchestrator-Instanz migriert, die in vRealize Automation eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Konfigurieren des integrierten vRealize Orchestrator -Servers

Nachdem Sie die Konfiguration eines externen Orchestrator-Servers exportiert und in vRealize Automation 7.4 importiert haben, müssen Sie den Orchestrator-Server konfigurieren, der in vRealize Automation integriert ist.

Voraussetzungen

Migrieren Sie die Konfiguration vom externen auf den internen vRealize Orchestrator-Server.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
- 2 Starten Sie den Control Center-Dienst und den Orchestrator-Serverdienst des integrierten vRealize Orchestrator-Servers.

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

- 3 Melden Sie sich beim Control Center des integrierten Orchestrator-Servers als **Administrator** an.

Hinweis Wenn Sie von einer externen vRealize Orchestrator 7.4-Instanz migrieren, fahren Sie mit Schritt 5 fort.

- 4 Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

- 5 Wenn der externe Orchestrator-Server für den Clustermodus konfiguriert wurde, konfigurieren Sie den Orchestrator-Cluster in vRealize Automation neu.
 - a Rufen Sie die Seite für die erweiterte **Verwaltung des Orchestrator-Clusters** unter `https://vra-va-Hostname.Domäne.Name_oder_Lastausgleichsadresse:8283/vco-controlcenter/#/control-app/ha?remove-nodes` auf.

Hinweis Wenn die Kontrollkästchen zum **Entfernen** neben den bestehenden Knoten im Cluster nicht angezeigt werden, müssen Sie die Browserseite aktualisieren, indem Sie auf der Tastatur die Funktionstaste F5 drücken.

 - b Aktivieren Sie die Kontrollkästchen neben den externen Orchestrator-Knoten und klicken Sie auf **Entfernen**, um sie aus dem Cluster zu entfernen.
 - c Wenn Sie die Seite für die erweiterte Verwaltung des Clusters verlassen möchten, löschen Sie die Zeichenfolge `remove-nodes` in der URL und aktualisieren Sie die Browserseite mit der Funktionstaste F5 auf der Tastatur.
 - d Prüfen Sie auf der Seite **Konfiguration überprüfen** im Control Center, ob Orchestrator ordnungsgemäß konfiguriert ist.
- 6 (Optional) Generieren Sie in der Registerkarte **Paketsignaturzertifikat** auf der Seite **Zertifikate** ein neues Paketsignaturzertifikat.
- 7 (Optional) Ändern Sie die Werte für **Standardmandant** und **Admin-Gruppe** auf der Seite **Anbieter für Authentifizierung konfigurieren**.
- 8 Stellen Sie sicher, dass der Dienst `vco-server` in der Registerkarte **Dienste** in der Managementkonsole der vRealize Automation-Appliance als REGISTRIERT angezeigt wird.
- 9 Wählen Sie die `vco`-Dienste des externen Orchestrator-Servers aus und klicken Sie auf **Registrierung aufheben**.

Nächste Schritte

- Importieren Sie alle vertrauenswürdigen Zertifikate aus dem externen Orchestrator-Server in den Trust Store des integrierten Orchestrator-Servers.
- Fügen Sie die vRealize Automation-Replikatknoten zum vRealize Automation-Cluster hinzu, um die Orchestrator-Konfiguration zu synchronisieren.

Weitere Informationen finden Sie in der Beschreibung der *Neukonfiguration der eingebetteten Zielinstanz von vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit* in *Installieren oder Upgrade von vRealize Automation*.

Hinweis Die vRealize Orchestrator-Instanzen werden automatisch zu Clustern zusammengefasst und stehen für die Verwendung zur Verfügung.

- Starten Sie den `vco-configurator`-Dienst auf allen Knoten im Cluster neu.
- Aktualisieren Sie den vRealize Orchestrator-Endpoint, um auf den migrierten integrierten Orchestrator-Server zu verweisen.

- Fügen Sie den vRealize Automation-Host und den IaaS-Host zur Bestandsliste des vRealize Automation-Plug-Ins hinzu, indem Sie die Workflows „Einen vRA-Host hinzufügen“ und „Den IaaS-Host eines vRA-Hosts hinzufügen“ ausführen.

Upgrade einer eigenständigen vRealize Orchestrator -Appliance für die Verwendung mit vRealize Automation

Wenn Sie eine eigenständige, externe Instanz von vRealize Orchestrator für die Verwendung mit vRealize Automation verwalten, müssen Sie vRealize Orchestrator bei einem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 aktualisieren.

Eingebettete Instanzen von vRealize Orchestrator werden als Teil der Aktualisierung der vRealize Automation-Appliance aktualisiert. Für eine eingebettete Instanz sind keine zusätzlichen Schritte erforderlich.

Informationen zum Aktualisieren eines vRealize Orchestrator-Appliance-Clusters finden Sie unter [Upgrade eines vRealize Orchestrator-Appliance-Clusters für die Verwendung mit vRealize Automation 7.4](#).

Voraussetzungen

- [Installieren des Updates auf der vRealize Automation-Appliance und den IaaS-Komponenten](#).
- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Erhöhen Sie den Arbeitsspeicher der vSphere Orchestrator-Appliance auf mindestens 6 GB. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Erstellen Sie einen Snapshot der virtuellen vSphere Orchestrator-Maschine. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in vSphere Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** im vSphere Control Center.

Verfahren

- ◆ Verwenden Sie eines der dokumentierten Verfahren, um Ihre eigenständige Instanz von vRealize Orchestrator zu aktualisieren.
 - [Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys](#).
 - [Aktualisieren von Orchestrator Appliance mithilfe eines ISO-Images](#).
 - [Upgrade von Orchestrator Appliance mithilfe eines angegebenen Repositorys](#).

Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys

Sie können Orchestrator zum Herunterladen des Upgrade-Pakets aus dem VMware-Standard-Repository konfigurieren.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.
- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter <https://Orchestrator-Server:5480> auf und melden Sie sich als **root** an.
- 2 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
Das Optionsfeld neben der Option **Standard-Repository verwenden** ist aktiviert.
- 3 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.
- 4 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.
- 5 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 6 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 7 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 8 Melden Sie sich beim Control Center als **root** an.
- 9 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

10 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Aktualisieren von Orchestrator Appliance mithilfe eines ISO-Images

Sie können Orchestrator zum Herunterladen eines Upgrade-Pakets aus einer ISO-Imagedatei konfigurieren, die sich auf dem CD-ROM-Laufwerk der Appliance befindet.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.
- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Laden Sie das Archiv `VMware-vRO-Appliance-Version-Build-Nummer-updaterepo.iso` von der offiziellen VMware-Downloadseite herunter.
- 2 Verbinden Sie das CD-ROM-Laufwerk der virtuellen Orchestrator Appliance-Maschine. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- 3 Stellen Sie die ISO-Imagedatei im CD-ROM-Laufwerk der Appliance bereit. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- 4 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter `https://Orchestrator-Server:5480` auf und melden Sie sich als **root** an.
- 5 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
- 6 Aktivieren Sie das Optionsfeld neben der Option **CD-ROM-Updates verwenden**.
- 7 Kehren Sie zur Seite **Status** zurück.
Die Version des verfügbaren Upgrades wird angezeigt.
- 8 Klicken Sie auf **Updates installieren**.
- 9 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 10 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 11 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 12 Melden Sie sich beim Control Center als **root** an.
- 13 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

14 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Upgrade von Orchestrator Appliance mithilfe eines angegebenen Repositorys

Sie können Orchestrator für die Verwendung eines lokalen Repositorys konfigurieren, in das Sie das Upgrade-Archiv hochgeladen haben.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.
- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Bereiten Sie das lokale Repository für Upgrades vor.
 - a Installieren und konfigurieren Sie einen lokalen Webserver.
 - b Laden Sie das Archiv `VMware-vRO-Appliance-Version-Build-Nummer-updaterepo.zip` von der offiziellen VMware-Downloadseite herunter.
 - c Extrahieren Sie das ZIP-Archiv in das lokale Repository.
- 2 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter `https://Orchestrator-Server:5480` auf und melden Sie sich als **root** an.
- 3 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
- 4 Aktivieren Sie das Optionsfeld neben der Option **Angegebenes Repository verwenden**.
- 5 Geben Sie die URL-Adresse des lokalen Repositories an, indem Sie das Verzeichnis `Update_Repo` angeben.
`http://Lokaler_Webserver:Port/build/mts/release/bora-Build-Nummer/publish/exports/Update_Repo`
- 6 Wenn für das lokale Repository eine Authentifizierung erforderlich ist, geben Sie den Benutzernamen und das Kennwort ein.
- 7 Klicken Sie auf **Einstellungen speichern**.
- 8 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.
- 9 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.
- 10 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 11 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 12 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 13 Melden Sie sich beim Control Center als **root** an.
- 14 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

15 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Upgrade eines vRealize Orchestrator -Appliance-Clusters für die Verwendung mit vRealize Automation 7.4

Wenn Sie einen vRealize Orchestrator-Appliance-Cluster mit vRealize Automation verwenden, müssen Sie ein Upgrade des Orchestrator-Appliance-Clusters auf Version 7.4 durchführen, indem Sie eine einzelne Instanz aktualisieren und neu installierte 7.4-Knoten mit der aktualisierten Instanz verbinden.

Informationen zum Upgrade einer einzelnen Instanz von vRealize Orchestrator finden Sie unter [Upgrade einer eigenständigen vRealize Orchestrator-Appliance für die Verwendung mit vRealize Automation](#).

Voraussetzungen

- [Installieren des Updates auf der vRealize Automation-Appliance und den IaaS-Komponenten](#).
- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Weitere Informationen finden Sie im [Konfigurationshandbuch für den Lastausgleich von vRealize Orchestrator](#).
- Erstellen Sie einen Snapshot aller vRealize Orchestrator-Serverknoten.
- Sichern Sie die gemeinsame vRealize Orchestrator-Datenbank.

Verfahren

- 1 Stoppen Sie auf allen Clusterknoten die Orchestrator-Dienste vco-server und vco-configurator.
- 2 Aktualisieren Sie nur eine Orchestrator-Serverinstanz in Ihrem Cluster mithilfe eines der dokumentierten Verfahren.

- 3 Stellen Sie eine neue Orchestrator Appliance in Version 7.3 bereit.
 - a Konfigurieren Sie den neuen Knoten mit den Netzwerkeinstellungen einer bereits vorhandenen Instanz, die Teil des Clusters ist, aber noch nicht aktualisiert wurde.
- 4 Rufen Sie das Control Center des zweiten Knotens auf, um den Konfigurationsassistenten zu starten.
 - a Navigieren Sie zu `https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.
- 5 Wählen Sie den Bereitstellungstyp **Orchestrator-Cluster** aus.

Durch die Auswahl dieses Typs wählen Sie aus, dass der Knoten einem vorhandenen Orchestrator-Cluster hinzugefügt werden soll.
- 6 Geben Sie in das Textfeld **Hostname** den Hostnamen oder die IP-Adresse der ersten Orchestrator-Serverinstanz ein.

Hinweis Hierbei muss es sich um die lokale IP-Adresse oder den Hostnamen der Orchestrator-Instanz handeln, der Sie den zweiten Knoten hinzufügen möchten. Verwenden Sie keine Lastausgleichsadresse.

- 7 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des Root-Benutzers für die erste Orchestrator-Serverinstanz ein.
- 8 Klicken Sie auf **Beitreten**. Die Orchestrator-Instanz kloniert die Konfiguration des Knotens, mit dem sie verbunden wird.

Der Orchestrator-Serverdienst beider Knoten wird automatisch neu gestartet.
- 9 Rufen Sie das Control Center des aktualisierten Orchestrator-Clusters über die Lastausgleichsadresse auf, und melden Sie sich als **Administrator** an.
- 10 Stellen Sie auf der Seite **Orchestrator-Clusterverwaltung** sicher, dass die Zeichenfolgen **Aktiver Konfigurationsfingerabdruck** und **Ausstehender Konfigurationsfingerabdruck** auf allen Knoten im Cluster übereinstimmen.

Hinweis Sie müssen die Seite möglicherweise mehrmals aktualisieren, bis die beiden Zeichenfolgen übereinstimmen.

- 11 Vergewissern Sie sich, dass der vRealize Orchestrator-Cluster ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** im Control Center öffnen.
- 12 (Optional) Wiederholen Sie die Schritte 3 bis 8 für jeden weiteren Knoten im Cluster.

Damit haben Sie den Orchestrator-Cluster aktualisiert.

Nächste Schritte

[Aktivieren der Lastausgleichsdienste.](#)

Aktivieren der Lastausgleichsdienste

Wenn Ihre Bereitstellung Lastausgleichsdienste verwendet, aktivieren Sie die sekundäre Knoten und Integritätsprüfungen erneut und stellen die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst wieder her.

Die Systemzustandsprüfungen für vRealize Automation variieren je nach Version. Informationen finden Sie im *vRealize Automation Load Balancing Configuration Guide* in der [VMware vRealize Automation-Dokumentation](#).

Setzen Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst von 10 Minuten zurück auf den Standardwert.

Aufgaben nach dem Upgrade von vRealize Automation

Nach dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 müssen Sie alle erforderlichen Aufgaben durchführen.

Upgrade von Software-Agents auf TLS 1.2

Nach der Migration auf vRealize Automation 7.4 müssen Sie verschiedene Aufgaben durchführen, um die Software-Agents von Ihrer vRealize Automation 7.1-, 7.2-, 7.3- oder 7.3.1-Umgebung auf TLS 1.2 zu aktualisieren.

Ab vRealize Automation 7.4 stellt Transport Layer Security (TLS) 1.2 das einzige unterstützte TLS-Protokoll für den Datenaustausch zwischen vRealize Automation und Ihrem Browser dar.

Nach der Migration müssen Sie vorhandene VM-Vorlagen aus Ihrer vRealize Automation 7.1-, 7.2-, 7.3- oder 7.3.1-Umgebung und alle vorhandenen virtuellen Maschinen aktualisieren.

Aktualisieren von vRealize Automation -VM-Vorlagen

Nach Abschluss des Upgrades auf vRealize Automation 7.4 müssen Sie vorhandene Vorlagen aktualisieren, damit die Software-Agents das TLS 1.2-Protokoll verwenden.

Gast-Agent- und Agent-Bootstrap-Code muss in den Vorlagen aus vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 aktualisiert werden. Wenn Sie eine Option mit verknüpftem Klon verwenden, müssen Sie die Vorlagen mit den neu erstellten virtuellen Maschinen und deren Snapshots möglicherweise neu zuordnen.

Um Ihre Vorlagen zu aktualisieren, führen Sie die folgenden Aufgaben durch.

- 1 Melden Sie sich bei vSphere an.
- 2 Konvertieren Sie jede Vorlage aus vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 in eine virtuelle Maschine und schaltet Sie die Maschine ein.
- 3 Importieren Sie das entsprechende Software-Installationsprogramm und führen Sie es auf jeder virtuellen Maschine aus.
- 4 Konvertieren Sie jede virtuelle Maschine zurück in eine Vorlage.

Wenden Sie dieses Verfahren bei der Suche nach dem Software-Installationsprogramm für Linux oder Windows an.

Voraussetzungen

Erfolgreiches Upgrade auf vRealize Automation 7.4

Verfahren

- 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation 7.4-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance: `https://vra-va-hostname.domain.name`.
- 2 Klicken Sie auf die **Gast- und Software-Agent-Seite**.
- 3 Befolgen Sie die Anweisungen für das Linux- oder Windows-Softwareinstallationsprogramm.

Nächste Schritte

[Identifizieren von virtuellen Maschinen, für die ein Software-Agent-Upgrade erforderlich ist.](#)

Identifizieren von virtuellen Maschinen, für die ein Software-Agent-Upgrade erforderlich ist

Sie können den Integritätsdienst in vRealize Automation verwenden, um virtuelle Maschinen zu identifizieren, für die ein Software-Agent-Update auf TLS 1.2 erforderlich ist.

Sie können den Integritätsdienst verwenden, um die virtuellen Maschinen zu identifizieren, für die ein Software-Agent-Update auf TLS 1.2 erforderlich ist. Alle Software-Agents in der vRealize Automation 7.4-Umgebung müssen aktualisiert werden, damit Sie nach erfolgter Bereitstellung Vorgänge durchführen können, für die eine sichere Kommunikation zwischen Ihrem Browser und vRealize Automation erforderlich ist.

Voraussetzungen

- Das Upgrade auf vRealize Automation 7.4 wurde erfolgreich durchgeführt.
- Sie sind bei vRealize Automation 7.4 auf der primären virtuellen Appliance als Mandantenadministrator angemeldet.

Verfahren

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

Option	Kommentar
Name	Geben Sie Software-Agent-Überprüfung ein.
Beschreibung	Fügen Sie optional eine Beschreibung hinzu. Beispiel: Software-Agents für Upgrade auf TLS 1.2 suchen.
Produkt	Wählen Sie vRealize Automation 7.4.0 aus.
Planen	Wählen Sie Keine aus.

- 4 Klicken Sie auf **Weiter**.

- 5 Wählen Sie auf der Seite „Testsuites auswählen“ die Optionen **Systemtests für vRealize Automation** und **Mandantentests für vRealize Automation** aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein.

Tabelle 1-56. Virtuelle vRealize Automation -Appliance

Option	Beschreibung
Adresse des öffentlichen Webservers	<ul style="list-style-type: none"> ■ Bei einer minimalen Bereitstellung ist dies die Basis-URL für den vRealize Automation-Appliance-Host. Beispielsweise <code>https://va-host.domain/</code>. ■ Bei einer High Availability-Bereitstellung ist dies die Basis-URL für den vRealize Automation-Lastausgleichsdienst. Beispiel: <code>https://load-balancer-host.domain/</code>.
Adresse der SSH-Konsole	Vollqualifizierter Domänenname der vRealize Automation-Appliance. Beispiel: <code>va-host.domain</code> .
Benutzer der SSH-Konsole	root
Kennwort der SSH-Konsole	Kennwort für Root.
Max. Antwortzeit für Dienst (ms)	Übernehmen Sie den Standardwert: 2000

Tabelle 1-57. vRealize Automation -Systemmandant

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

Tabelle 1-58. vRealize Automation -Festplattenspeicherüberwachung

Option	Beschreibung
Warnschwellenwert (in Prozent)	Übernehmen Sie den Standardwert: 75
Kritischer Schwellenwert (in Prozent)	Übernehmen Sie den Standardwert: 90

Tabelle 1-59. vRealize Automation -Mandant

Option	Beschreibung
Zu testender Mandant	Zu Testzwecken ausgewählter Mandant.
Benutzername des Fabric-Administrators	Benutzername des Fabric-Administrators. Beispiel: <code>admin@va-host.local</code> . Hinweis Dieser Fabric-Administrator muss auch über eine Mandantenadministrator- und eine IaaS-Administratorrolle verfügen, um alle Tests ausführen zu können.
Kennwort des Fabric-Administrators	Kennwort des Fabric-Administrators.

- 8 Klicken Sie auf **Weiter**.

- 9 Überprüfen Sie die Informationen auf der Seite „Übersicht“ und klicken Sie auf **Beenden**.
Die Konfiguration der Software-Agent-Überprüfung ist abgeschlossen.
- 10 Klicken Sie auf der Karte für die Software-Agent-Überprüfung auf **Ausführen**.
- 11 Wenn der Test abgeschlossen ist, klicken Sie auf die Mitte der Karte für die Software-Agent-Überprüfung.
- 12 Navigieren Sie auf der Ergebnisseite der Software-Agent-Überprüfung durch die Testergebnisse und suchen Sie den Test für die Software-Agent-Version in der Spalte „Name“. Wenn das Testergebnis „Fehlgeschlagen“ lautet, klicken Sie in der Spalte „Ursache“ auf den Link **Ursache**, um die virtuellen Maschinen mit veralteten Software-Agents anzuzeigen.

Nächste Schritte

Wenn Sie über virtuelle Maschinen mit einem veralteten Software-Agent verfügen, finden Sie weitere Informationen unter [Upgrade von Software-Agents auf vSphere](#).

Upgrade von Software-Agents auf vSphere

Nach dem Upgrade können Sie beliebige veraltete Software-Agents auf vSphere auf TLS 1.2 aktualisieren. Verwenden Sie hierfür die Verwaltungsschnittstelle der vRealize Automation-Appliance.

Bei diesem Verfahren werden die veralteten Software-Agents auf den virtuellen Maschinen in Ihrer aktualisierten Umgebung auf TLS 1.2 aktualisiert. Dieses Verfahren ist auch für das Upgrade auf vRealize Automation 7.4 erforderlich.

Voraussetzungen

- Erfolgreiches Upgrade auf vRealize Automation 7.4
- Sie haben den Integritätsdienst verwendet, um virtuelle Appliances mit veralteten Software-Agents zu identifizieren.

Verfahren

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
Öffnen Sie in einer Hochverfügbarkeitsumgebung die Verwaltungsschnittstelle der Appliance auf der Master-Appliance.
- 2 Klicken Sie auf **vRA-Einstellungen > SW-Agents**.
- 3 Klicken Sie auf **TLS 1.0, 1.1 aktivieren und deaktivieren**.
Der Status von TLS v1.0, v1.1 lautet AKTIVIERT.

- 4 Geben Sie für die Mandantenanmeldedaten die angeforderten Informationen für die vRealize Automation 7.4-Appliance ein.

Option	Beschreibung
Mandantenname	Name des Mandanten auf der aktualisierten vRealize Automation-Appliance. Hinweis Die Mandantenbenutzer muss über die zugewiesene Rolle „Softwarearchitekt“ verfügen.
Benutzername	Benutzername des Mandantenadministrators auf der vRealize Automation-Appliance.
Kennwort	Kennwort des Mandantenadministrators.

- 5 Klicken Sie auf **Testverbindung**.

Wenn eine Verbindung hergestellt werden konnte, wird eine Erfolgsmeldung angezeigt.

- 6 Klicken Sie auf **Batches auflisten**.

Die Tabelle „Batch-Auswahlliste“ wird angezeigt.

- 7 Klicken Sie auf **Anzeigen**.

Eine Tabelle mit einer Liste von virtuellen Maschinen mit veralteten Software-Agents wird angezeigt.

- 8 Aktualisieren Sie den Software-Agent für die virtuellen Maschinen, die sich im Zustand AKTUALISIERBAR befinden.

- Um den Software-Agent in einer einzelnen virtuellen Maschine zu aktualisieren, klicken Sie für eine Gruppe von virtuellen Maschinen auf **Anzeigen**, identifizieren Sie die virtuelle Maschine, die Sie aktualisieren möchten, und klicken Sie auf **Ausführen**, um das Upgrade zu starten.
- Um den Software-Agent für eine Gruppe von virtuellen Maschinen zu aktualisieren, identifizieren Sie die zu aktualisierende Gruppe und klicken Sie auf **Ausführen**, um das Upgrade zu starten.

Wenn Sie mehr als 200 virtuelle Maschinen aktualisieren möchten, können Sie die Geschwindigkeit des Batch-Upgrades durch Eingabe von Werten für diese Parameter steuern.

Option	Beschreibung
Batchgröße	Die für das Batch-Upgrade ausgewählte Anzahl der virtuellen Maschinen. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.
Warteschlangentiefe	Die Anzahl der parallelen Upgrades, die gleichzeitig ausgeführt werden können. Beispielsweise 20. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.
Batchfehler	Die Anzahl der REST-Fehler, die zur Verlangsamung des Batch-Upgrades führt. Beispiel: Wenn Sie das aktuelle Batch-Upgrade nach 5 Fehlern stoppen möchten, um die Stabilität des Upgrades zu verbessern, geben Sie „5“ in das Textfeld ein.

Option	Beschreibung
Batchausfälle	Die Anzahl der fehlgeschlagenen Software-Agent-Upgrades, die dazu führt, dass die Batchverarbeitung verlangsamt wird. Beispiel: Wenn Sie das aktuelle Batch-Upgrade nach 5 Fehlern stoppen möchten, um die Stabilität des Upgrades zu verbessern, geben Sie „5“ in das Textfeld ein.
Batchabruf	Wie oft der Upgradevorgang abgefragt wird, um den Status des Upgrades zu überprüfen. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.

Wenn der Upgradevorgang zu langsam ist oder zu viele nicht erfolgreiche Upgrades erzeugt, können Sie diese Parameter anpassen, um die Upgradeleistung zu verbessern.

Hinweis Durch Klicken auf **Aktualisieren** wird die Liste der Batches gelöscht. Dieser Schritt wirkt sich nicht auf den Upgradevorgang aus. Zudem werden Informationen darüber aktualisiert, ob TLS 1.2 festgelegt ist oder nicht. Darüber hinaus wird beim Klicken auf **Aktualisieren** auch eine Integritätsprüfung der vRealize Automation-Dienste durchgeführt. Wenn Dienste nicht ausgeführt werden, zeigt das System eine Fehlermeldung an und alle anderen Aktionsschaltflächen werden deaktiviert.

9 Klicken Sie auf **TLS 1.0, 1.1 aktivieren und deaktivieren**.

Der Status von TLS v1.0, v1.1 lautet DEAKTIVIERT.

Upgrade von Software-Agents auf Amazon Web Service oder Azure

Sie können beliebige veraltete Software-Agents auf virtuellen Maschinen auf Amazon Web Service (AWS) oder Azure manuell aktualisieren.

Voraussetzungen

- Erfolgreiches Upgrade auf vRealize Automation 7.4
- Ein Softwaretunnel ist vorhanden und die IP-Adresse der virtuellen Maschine im Tunnel ist bekannt.

Verfahren

1 Erstellen Sie eine Knotendatei für jeden Knoten, für den Sie ein Upgrade durchführen müssen.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

Hinweis Bei einem direkten Upgrade ist der \$DestinationVRAServer identisch mit dem \$SourceVRAServer.

2 Erstellen Sie eine Plandatei, um den Software-Agent auf einer Linux- oder Windows-VM zu aktualisieren.

- Ändern Sie die Datei für die Migration von Parametern unter „/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}“ so, dass diese den Wert der privaten IP-Adresse entsprechend dem AWS- oder Azure-Endpoint enthält.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
```

- Verwenden Sie diesen Befehl für die Aktualisierung einer Linux-Maschine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --sour-
ce_cloud_provider azure
```

- Verwenden Sie diesen Befehl für die Aktualisierung einer Windows-Maschine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --sour-
ce_cloud_provider azure
```

- Mit diesem Befehl wird die Plandatei ausgeführt.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Verwenden Sie diesen Befehl, um den Software-Agent mit der Knotendatei aus Schritt 1 und der Plandatei aus Schritt 2 zu aktualisieren.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Als Alternative können Sie diesen Befehl verwenden, um über die Knotendatei nur jeweils einen Knoten auszuführen. Geben Sie hierfür einen Knotenindex an.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Wenn Sie diesen Vorgang ausführen, können Sie den Protokollen aus der virtuellen vRealize Automation-Appliance und der Hostmaschine folgen, um den Fortschritt des Server-Agent-Upgrades anzuzeigen.

Nach dem Upgrade importiert der Upgradevorgang ein Softwareaktualisierungsskript für Windows oder Linux auf die virtuelle vRealize Automation 7.4-Appliance. Sie können sich bei dem virtuellen vRealize Automation-Appliance-Host anmelden, um sicherzustellen, dass die Softwarekomponente erfolgreich importiert wurde. Nach dem Importieren der Komponente wird eine Softwareaktualisierung an den Event Broker Service (EBS) gesendet, um die Softwareaktualisierungsskripte an die identifizierten virtuellen Maschinen weiterzuleiten. Wenn das Upgrade abgeschlossen ist und die neuen Software-Agents betriebsbereit sind, werden sie durch das Senden einer Ping-Anforderung an die neue virtuelle vRealize Automation-Appliance gebunden.

Hinweis Nützliche Protokolldateien

- Catalina-Ausgabe für Quell-vRealize Automation: `/var/log/vcac/catalina.out`. In dieser Datei stellen Sie fest, dass die Upgrade-Anforderungen während der Agent-Migrationen vorgenommen wurden. Diese Aktivität ist mit der Ausführung einer Software-Bereitstellungsanforderung identisch.
- Catalina-Ausgabe für Ziel-vRealize Automation: `/var/log/vcac/catalina.out`. In dieser Datei werden die Ping-Anforderungen der migrierten virtuellen Maschinen mit den 7.4.0-SNAPSHOT-Versionsnummern angegeben. Sie können diese berechnen, indem Sie die EBS-Themennamen vergleichen, z. B. `sw-agent-UUID`.
- Agent-Aktualisierungsordner in der Protokolldatei für das Master-Upgrade der zieleitigen vRealize Automation-Maschine: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. Mit dieser Datei können Sie nachverfolgen, welcher Upgradevorgang derzeit ausgeführt wird.

- Einzelne in Mandantenordnern verfügbare Protokolle: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Einzelne Knoten werden hier als LOT-Dateien mit Fehlern und laufenden Erweiterungen angezeigt.
- Migrierte VMs: `/opt/vmware-appdirector/agent/logs/darwin*.log`. Sie können diesen Speicherort, der die empfangenen Software-Aktualisierungsanforderungen sowie einen eventuellen Neustart des Agent-Bootstrap und Software-Agent auflistet, stichprobenhaft überprüfen.

Festlegen des vRealize Automation PostgreSQL-Replikatmodus auf „synchron“

Wenn Sie den PostgreSQL-Replikatmodus vor dem Upgrade auf „asynchron“ festlegen, können Sie den PostgreSQL-Replikatmodus nach dem Upgrade einer verteilten vRealize Automation-Umgebung auf „synchron“ festlegen.

Voraussetzungen

- Sie haben eine verteilte vRealize Automation-Umgebung aktualisiert.
- Sie sind als **Root-Benutzer** bei der Verwaltungsschnittstelle der entsprechenden vRealize Automation-Appliance (<https://vra-va-hostname.domain.name:5480>) angemeldet.

Verfahren

- 1 Klicken Sie auf **vRA-Einstellungen > Datenbank**.
- 2 Klicken Sie auf **Sync-Modus** und warten Sie, bis die Aktion abgeschlossen ist.
- 3 Stellen Sie sicher, dass alle Knoten in der Spalte „Synchronisierungsstatus“ den Status Sync anzeigen.

Nächste Schritte

[Ausführen einer Testverbindung und Überprüfen von aktualisierten Endpoints.](#)

Ausführen einer Testverbindung und Überprüfen von aktualisierten Endpoints

Beim Upgrade von vRealize Automation 7.3 oder früher auf 7.4 werden Änderungen an Endpoints in der Zielumgebung vorgenommen.

Nach dem Upgrade auf vRealize Automation 7.4 müssen Sie die Aktion **Testverbindung** für alle anwendbaren Endpoints durchführen. Außerdem müssen Sie möglicherweise einige aktualisierte Endpoints anpassen. Weitere Informationen finden Sie unter [Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints](#).

Die Standardsicherheitseinstellung für aktualisierte oder migrierte Endpoints ist, nicht vertrauenswürdige Zertifikate nicht zu akzeptieren.

Wenn Sie nicht vertrauenswürdige Zertifikate verwendet haben, müssen Sie nach dem Upgrade oder der Migration von einer früheren vRealize Automation-Installation die folgenden Schritte für alle vSphere- und NSX-Endpoints ausführen, um die Validierung des Zertifikats durchzuführen. Andernfalls schlagen die Endpoint-Vorgänge mit Zertifikatsfehlern fehl. Weitere Informationen finden Sie in den VMware Knowledgebase-Artikeln *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* unter <http://kb.vmware.com/kb/2150230> und *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* unter <http://kb.vmware.com/kb/2108294>.

- 1 Melden Sie sich nach dem Upgrade bzw. der Migration bei der vRealize Automation vSphere-Agent-Maschine an und starten Sie Ihre vSphere-Agents mithilfe der Registerkarte **Dienste** neu.
Im Fall einer Migration werden möglicherweise nicht alle Agents neu gestartet. Starten Sie diese bei Bedarf manuell neu.
- 2 Warten Sie, bis mindestens ein Ping-Bericht abgeschlossen ist. Es dauert eine oder zwei Minuten, bis ein Ping-Bericht abgeschlossen ist.
- 3 Wenn die vSphere-Agents die Datenerfassung gestartet haben, melden Sie sich bei vRealize Automation als IaaS-Administrator an.
- 4 Klicken Sie auf **Infrastruktur > Endpoints > Endpoints**.
- 5 Bearbeiten Sie einen vSphere-Endpoint und klicken Sie auf **Verbindung testen**.
- 6 Wenn eine Zertifikataufforderung angezeigt wird, klicken Sie auf **OK**, um das Zertifikat zu akzeptieren.
Wenn keine Zertifikataufforderung angezeigt wird, kann es sein, dass das Zertifikat derzeit korrekt in einer vertrauenswürdigen Rootzertifizierungsstelle der Windows-Maschine gespeichert ist, die Dienste für den Endpoint hostet, z. B. als Proxy-Agent-Maschine oder DEM-Maschine.
- 7 Klicken Sie auf **OK**, um die Zertifikatsannahme anzuwenden und den Endpoint zu speichern.
- 8 Wiederholen Sie diesen Vorgang für jeden vSphere-Endpoint.
- 9 Wiederholen Sie diesen Vorgang für jeden NSX-Endpoint.

Wenn die Aktion **Verbindung testen** erfolgreich war, aber einige Datenerfassungs- bzw. Bereitstellungsvorgänge fehlschlagen, können Sie dasselbe Zertifikat auf allen Agent-Maschinen installieren, die den Endpoint bedienen, sowie auf allen DEM-Maschinen. Alternativ dazu können Sie das Zertifikat von vorhandenen Maschinen deinstallieren und den oben genannten Vorgang für den fehlerhaften Endpoint wiederholen.

Durchführen der Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste nach dem Upgrade von vRealize Automation

Nach dem Upgrade von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4 müssen Sie in der vRealize Automation 7.4-Umgebung eine Datenerfassung für die NSX-Netzwerk- und Sicherheitsbestandsliste durchführen.

Diese Datenerfassung ist erforderlich, damit die Neukonfiguration des Lastausgleichs in vRealize Automation 7.4 für 7.1-, 7.2- oder 7.3.x-Bereitstellungen möglich ist.

Voraussetzungen

- [Durchführen der Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste vor dem vRealize Automation-Upgrade.](#)
- Erfolgreiches Upgrade auf vRealize Automation 7.4

Verfahren

- ◆ Führen Sie nach dem Upgrade eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in vRealize Automation 7.4 durch. Weitere Informationen finden Sie unter [Manuelles Starten der Endpoint-Datenerfassung](#).

Verknüpfen der Replikat-Appliance mit dem Cluster

Nach dem Update der Master-vRealize Automation-Appliance wird jeder aktualisierte Replikatknoten automatisch mit dem Master-Knoten verknüpft. Falls ein Replikat-Knoten separat aktualisiert werden muss, verknüpfen Sie den Replikat-Knoten anhand der folgenden Schritte mit dem Cluster.

Greifen Sie auf die Verwaltungskonsole des Replikat-Knotens zu, der nicht mit dem Cluster verknüpft ist, und führen Sie folgende Schritte durch.

Verfahren

- 1 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 2 Klicken Sie auf **Cluster beitreten**.

Portkonfiguration für Hochverfügbarkeitsbereitstellungen

Nach einem Upgrade in einer Hochverfügbarkeitsbereitstellung müssen Sie den Lastausgleichsdienst so konfigurieren, dass der Datenverkehr an Port 8444 an die vRealize Automation-Appliance geleitet wird, um Remote-Konsolenfunktionen zu unterstützen.

Weitere Informationen finden Sie im *vRealize Automation Load Balancing Configuration Guide* in der [vRealize Automation-Dokumentation](#).

Neukonfigurieren des integrierten vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit

Für eine Hochverfügbarkeitsbereitstellung müssen Sie jede zweiseitige Replikat-Appliance von vRealize Automation mit dem Cluster verbinden, damit die Hochverfügbarkeit für den eingebetteten vRealize Orchestrator unterstützt wird.

Voraussetzungen

Melden Sie sich bei der zweiseitigen Verwaltungskonsole der vRealize Automation-Replikat-Appliance an.

- 1 Starten Sie einen Browser und öffnen Sie die Verwaltungskonsole der zweiseitigen Replikat-vRealize Automation-Appliance mithilfe des vollqualifizierten Domänennamens (FQDN) der zweiseitigen virtuellen Replikat-Appliance: `https://vra-va-hostname.domain.name:5480`.
- 2 Melden Sie sich mit dem beim Bereitstellen der zweiseitigen Replikat-vRealize Automation-Appliance eingegebenen Benutzernamen **Root** und dem zugehörigen Kennwort an.

Verfahren

- 1 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 2 Geben Sie in das Textfeld **Führender Clusterknoten** den FQDN der zieleitigen vRealize Automation-Master-Appliance an.
- 3 Geben Sie das Root-Kennwort in das Textfeld **Kennwort** ein.
- 4 Klicken Sie auf **Cluster beitreten**.

Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort. Das System startet die Dienste für den Cluster neu.

- 5 Stellen Sie sicher, dass alle Dienste ausgeführt werden.
 - a Klicken Sie auf der obersten Registerkartenleiste auf **Dienste**.
 - b Klicken Sie auf **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Wiederherstellen von Dateien für die Zeitüberschreitung bei externen Workflows

Sie müssen die Dateien für die Zeitüberschreitung bei externen Workflows in vRealize Automation neu konfigurieren, da der Upgradevorgang die XMLDB-Dateien überschreibt.

Verfahren

- 1 Öffnen Sie die Konfigurationsdateien für den externen Workflow (xmlldb) auf dem System über das folgende Verzeichnis.
`\\VMware\vCAC\Server\ExternalWorkflows\xmlldb\.`
- 2 Ersetzen Sie die XMLDB-Dateien durch die Dateien, die Sie vor der Migration gesichert haben. Wenn Sie über keine Sicherungsdateien verfügen, konfigurieren Sie die Einstellungen für die Zeitüberschreitung bei externen Workflows.
- 3 Speichern Sie Ihre Einstellungen.

Aktivieren der Aktion „Mit Remote-Konsole verbinden“ für Verbraucher

Die Remote-Konsolen-Aktion für Verbraucher wird für Appliances unterstützt, die von vSphere in vRealize Automation bereitgestellt werden.

Bearbeiten Sie den Blueprint, nachdem Sie ein Versions-Upgrade ausgeführt haben, und wählen Sie die Aktion **Mit Remote-Konsole verbinden** auf der Registerkarte **Aktion** aus.

Weitere Informationen finden Sie im [Knowledgebase-Artikel 2109706](#).

Wiederherstellung von vorgenommenen Änderungen an der Protokollierung in der app.config-Datei

Der Upgrade-Vorgang überschreibt Änderungen, die Sie an der Protokollierung vornehmen, in den Konfigurationsdateien. Nach Abschluss eines Upgrades müssen Sie alle Änderungen wiederherstellen, die Sie vor dem Upgrade an der Datei `app.config` vorgenommen haben.

Aktivieren des automatischen Manager Service-Failovers nach einem Upgrade

Das automatische Manager Service-Failover ist standardmäßig deaktiviert, wenn Sie vRealize Automation aktualisieren.

Führen Sie diese Schritte durch, um das automatische Manager Service-Failover nach einem Upgrade zu aktivieren.

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung als Root-Benutzer auf der vRealize Automation-Appliance.
- 2 Wechseln Sie zum Verzeichnis `/usr/lib/vcac/tools/vami/commands`.
- 3 Um das automatische Manager Service-Failover zu aktivieren, führen Sie den folgenden Befehl aus.

```
python ./manager-service-automatic-failover ENABLE
```

Um das automatische Failover in der gesamten IaaS-Bereitstellung zu deaktivieren, führen Sie den folgenden Befehl aus.

```
python ./manager-service-automatic-failover DISABLE
```

Informationen zum automatischen Manager Service-Failover

Sie können den vRealize Automation IaaS Manager Service so konfigurieren, dass automatisch ein Failover zu einem Backup durchgeführt wird, wenn der primäre Manager Service beendet wird.

Ab vRealize Automation 7.3 müssen Sie den Manager Service nicht mehr auf jedem Windows-Server manuell starten oder beenden, um zu steuern, welcher Server als primärer Server oder als Backup dient. Das automatische Manager Service-Failover ist standardmäßig deaktiviert, wenn Sie das Upgrade von IaaS mit dem Upgrade-Shell-Skript oder mit der ausführbaren Datei für das IaaS-Installationsprogramm durchführen.

Wenn automatisches Failover aktiviert ist, wird der Manager Service automatisch auf allen Manager Service-Hosts, einschließlich der Backups, gestartet. Die automatische Failover-Funktion ermöglicht die gegenseitige transparente Überwachung der Hosts und die Durchführung eines Failovers bei Bedarf. Der Windows-Dienst muss jedoch auf allen Hosts ausgeführt werden.

Hinweis Es ist nicht erforderlich, automatisches Failover zu verwenden. Sie können diese Funktion deaktivieren und den Windows-Dienst weiterhin manuell starten und beenden, um zu steuern, welcher Host als primärer Host oder als Backup dient. Beim manuellen Failover müssen Sie den Dienst nur jeweils auf einem Host starten. Bei deaktiviertem automatischem Failover führt die gleichzeitige Ausführung des Diensts auf mehreren IaaS-Servern dazu, dass vRealize Automation nicht mehr verwendet werden kann.

Versuchen Sie nicht, automatisches Failover selektiv zu aktivieren oder zu deaktivieren. Automatisches Failover muss immer auf jedem Manager Service-Host in einer IaaS-Bereitstellung als aktiviert oder deaktiviert synchronisiert werden.

Fehlerbehebung bei vRealize Automation -Upgrades

Die Themen zur Fehlerbehebung bei einem Upgrade bieten Lösungen für Probleme, die beim Aktualisieren von vRealize Automation 7.1, 7.2 oder 7.3.x auf 7.4. auftreten können.

Das automatische Manager Service-Failover wird nicht aktiviert

Empfehlungen zur Fehlerbehebung des Befehls `manager-service-automatic-failover`.

Lösung

- Der Befehl zum Aktivieren des automatischen Manager Service-Failovers schlägt fehl oder zeigt diese Nachricht länger als zwei Minuten an: Das automatische Manager Service-Failover wird auf folgendem Knoten aktiviert: `IAAS_MANAGER_SERVICE_NODEID`.
 - a Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance unter `https://va-hostname.domain.name:5480` mit dem Benutzernamen **host** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance eingegeben haben.
 - b Wählen Sie **vRA-Einstellungen > Cluster** aus.
 - c Stellen Sie sicher, dass der Management-Agent-Dienst auf allen Manager Service-Hosts ausgeführt wird.
 - d Stellen Sie sicher, dass die Dauer der letzten Verbindung für alle IaaS-Manager Service-Knoten weniger als 30 Sekunden beträgt.

Wenn Sie Verbindungsprobleme bei einem Management-Agent feststellen, beheben Sie diese manuell und wiederholen Sie den Befehl zum Aktivieren des automatischen Manager Service-Failovers.

- Der Befehl zum Aktivieren des automatischen Manager Service-Failovers kann das Failover auf einem Manager Service-Knoten nicht aktivieren. Führen Sie den Befehl erneut aus, um dieses Problem zu beheben.
- Für einige Manager Service-Hosts in der IaaS-Bereitstellung wurde das Failover aktiviert, für andere nicht. Die Funktion muss für alle Manager Service-Hosts in der IaaS-Bereitstellung aktiviert werden, damit sie korrekt funktioniert. Um dieses Problem zu beheben, gehen Sie wie folgt vor:
 - Deaktivieren Sie das Failover auf allen Manager Service-Knoten und verwenden Sie stattdessen das manuelle Failover. Führen Sie das Failover nicht auf mehreren Hosts gleichzeitig aus.
 - Wenn mehrere Versuche, die Funktion auf einem Manager Service-Knoten zu aktivieren, fehlschlagen, beenden Sie den Windows VMware vCloud Automation Center-Dienst auf diesem Knoten und ändern Sie den Starttyp für den Knoten auf „Manuell“, bis Sie das Problem behoben haben.
- Verwenden Sie Python, um zu bestätigen, dass das Failover auf jedem Manager Service-Knoten aktiviert ist.
 - a Melden Sie sich beim Masterknoten der vRealize Automation-Appliance mithilfe von SSH als **root** an.

- b Führen Sie `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE` aus.
- c Stellen Sie sicher, dass das System diese Meldung ausgibt: Das automatische Manager Service-Failover wird auf folgendem Knoten aktiviert: `IAAS_MANAGER_SERVICE_NODEID` durchgeführt.
- Überprüfen Sie, ob das Failover auf jedem Manager Service-Knoten aktiviert ist, indem Sie die Konfigurationsdatei des Manager Service prüfen.
 - a Öffnen Sie eine Eingabeaufforderung auf einem Manager Service-Knoten.
 - b Rufen Sie den Installationsordner für vRealize Automation auf und öffnen Sie die Manager Service-Konfigurationsdatei unter `VMware\VCAC\Server\ManagerService.exe.config`.
 - c Stellen Sie sicher, dass die folgenden Elemente im Abschnitt `<appSettings>` vorhanden sind.
 - `<add key="FailoverModeEnabled" value="True" />`
 - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
 - `<add key="FailoverNodeState" value="active" />`
 - `<add key="FailoverMaxFailedDatabasePingAttempts" value="5" />`
 - `<add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />`
- Stellen Sie sicher, dass der Status des Windows VMware vCloud Automation Center-Dienstes „Gestartet“ lautet und als Starttyp „Automatisch“ eingestellt ist.
- Verwenden Sie Python, um zu bestätigen, dass das Failover auf jedem Manager Service-Knoten deaktiviert ist.
 - a Melden Sie sich beim Masterknoten der vRealize Automation-Appliance mithilfe von SSH als **root** an.
 - b Führen Sie `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE` aus.
 - c Stellen Sie sicher, dass das System diese Meldung ausgibt: Das automatische Manager Service-Failover wird auf folgendem Knoten deaktiviert: `IAAS_MANAGER_SERVICE_NODEID` durchgeführt.
- Überprüfen Sie, ob das Failover auf allen Manager Service-Knoten deaktiviert wurde, indem Sie die Manager Service-Konfigurationsdatei überprüfen.
 - a Öffnen Sie eine Eingabeaufforderung auf einem Manager Service-Knoten.
 - b Rufen Sie den Installationsordner für vRealize Automation auf und öffnen Sie die Manager Service-Konfigurationsdatei unter `VMware\VCAC\Server\ManagerService.exe.config`.
 - c Stellen Sie sicher, dass das folgende Element im Abschnitt `<appSettings>` vorhanden ist.
 - `<add key="FailoverModeEnabled" value="False" />`
- Um einen Cold-Standby-Manager Service-Knoten zu erstellen, beenden Sie den Windows VMware vCloud Automation Center-Dienst für den Knoten und ändern Sie den Starttyp in „Manuell“.

- Für einen aktiven Manager Service-Knoten muss der Windows VMware vCloud Automation Center-Dienst ausgeführt und als Starttyp „Automatisch“ festgelegt werden.
- Der Befehl zum Aktivieren des automatischen Manager Service-Failovers verwendet die interne ID des Manager Service-Knotens, *IAAS_MANAGER_SERVICE_NODEID*. Um den Hostnamen dieser internen ID zu finden, führen Sie den Befehl `vra-command list-nodes` aus und suchen Sie nach dem Manager Service-Host mit der Knoten-ID *IAAS_MANAGER_SERVICE_NODEID*.
- Um den Manager Service zu finden, den das System automatisch als „derzeit aktiv“ ausgewählt hat, führen Sie diese Schritte aus.
 - a Melden Sie sich beim Masterknoten der vRealize Automation-Appliance mithilfe von SSH als **root** an.
 - b Führen Sie `vra-command list-nodes --components` aus.
 - Wenn das Failover aktiviert ist, suchen Sie den Manager Service-Knoten mit dem Status „Aktiv“.
 - Wenn das Failover deaktiviert ist, suchen Sie den Manager Service-Knoten mit dem Status: „Gestartet“.

Installations- oder Aktualisierungsfehler mit einem Zeitüberschreitungsfehler des Lastausgleichsdiensts

Ein(e) vRealize Automation-Installation bzw. -Upgrade für eine verteilte Bereitstellung mit einem Lastausgleichsdienst schlägt mit Fehler 503 „Dienst nicht verfügbar“ fehl.

Problem

Die Installation bzw. das Upgrade schlägt fehl, da der Zeitüberschreitungswert für den Lastausgleichsdienst nicht genügend Zeit zum Abschluss der Aufgabe einräumt.

Ursache

Ein unzureichender Zeitüberschreitungswert für den Lastausgleichsdienst kann zu einem Fehler führen. Sie können das Problem beheben, indem Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden erhöhen und die Aufgabe erneut ausführen.

Lösung

- 1 Erhöhen Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden.
- 2 Führen Sie die Installation bzw. das Upgrade erneut aus.

Upgrade für die IaaS-Website-Komponente schlägt fehl

Das IaaS-Upgrade schlägt fehl und Sie können das Upgrade nicht fortsetzen.

Problem

Das laas-Upgrade schlägt für die Website-Komponente fehl. Die folgenden Fehlermeldungen werden in der Protokolldatei des Installationsprogramms angezeigt.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

Die folgenden Fehlermeldungen werden in der Repository-Protokolldatei angezeigt.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at

```
System.Data.Common.Internal.Materialization.Shaper`1.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core-
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Ursache

Das IaaS-Upgrade schlägt fehl, wenn das Erstellungsdatum für die Datei `web.config` dasselbe oder ein späteres ist als das Datum der Änderung.

Lösung

- 1 Melden Sie sich auf dem IaaS-Host bei Windows an.
- 2 Öffnen Sie die Windows-Eingabeaufforderung.
- 3 Wechseln Sie zum vRealize Automation-Installationsverzeichnis.
- 4 Starten Sie Ihren bevorzugten Text-Editor mit der Option **Als Administrator ausführen**.
- 5 Suchen und wählen Sie die Datei `web.config` aus und speichern Sie die Datei, um das Änderungsdatum zu ändern.
- 6 Überprüfen Sie die Eigenschaften der Datei `web.config`, um zu bestätigen, dass das Änderungsdatum hinter dem Erstellungsdatum liegt.
- 7 Führen Sie ein Upgrade von IaaS aus.

Manager Service kann aufgrund von SSL-Validierungsfehlern während der Laufzeit nicht ausgeführt werden

Der Manager Service kann aufgrund von SSL-Validierungsfehlern nicht ausgeführt werden.

Problem

Der Manager Service kann nicht ausgeführt werden und im Protokoll wird die folgende Fehlermeldung angezeigt:

[Info]: Thread-Id="6" – context="" token="" Fehler beim Verbinden mit der Hauptdatenbank, erneuter Versuch in 00:00:05, Fehlerdetails: Eine Verbindung mit dem Server wurde erfolgreich hergestellt, aber dann ist während des Anmeldevorgangs ein Fehler aufgetreten. (Anbieter: SSL-Anbieter, Fehler: 0 – Die Zertifikatkette wurde von einer Autorität ausgestellt, der nicht vertraut wird.)

Ursache

Während der Laufzeit kann der Manager Service aufgrund von SSL-Validierungsfehlern nicht ausgeführt werden.

Lösung

- 1 Öffnen Sie die Konfigurationsdatei `ManagerService.config`.
- 2 Aktualisieren Sie in der folgenden Zeile die entsprechende Einstellung auf **Encrypt=False**:

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Fehlschlagen der Anmeldung nach dem Upgrade

Nach einem Upgrade müssen Sie für die Sitzungen den Browser beenden und sich neu anmelden, die nicht synchronisierte Benutzerkonten verwenden.

Problem

Nach dem Upgrade von vRealize Automation verweigert das System bei der Anmeldung den Zugriff auf nicht synchronisierte Benutzerkonten.

Lösung

Beenden Sie den Browser und starten Sie vRealize Automation neu.

Löschen von verwaisten Knoten in vRealize Automation

Ein verwaister Knoten ist ein doppelter Knoten, der auf dem Host gemeldet wird, aber auf dem Host nicht existiert.

Problem

Wenn Sie überprüfen, ob sich alle IaaS- und virtuellen Appliance-Knoten in fehlerfreiem Zustand befinden, stellen Sie möglicherweise fest, dass es auf einem Host einen oder mehrere verwaiste Knoten gibt. Sie müssen alle verwaisten Knoten löschen.

Lösung

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 2 Wählen Sie **vRA-Einstellungen > Cluster** aus.

3 Klicken Sie für jeden verwaisten Knoten in der Tabelle auf **Löschen**.

Befehl „Cluster beitreten“ schlägt scheinbar fehl nach einem Upgrade einer Hochverfügbarkeitsumgebung

Nachdem Sie in der Managementkonsole eines sekundären Cluster-Knotens auf **Cluster beitreten** geklickt haben, wird die Statusanzeige nicht mehr angezeigt.

Problem

Wenn Sie die Verwaltungskonsole der vRealize Automation-Appliance nach dem Upgrade verwenden, um einen sekundären Clusterknoten zum primären Knoten hinzuzufügen, wird die Statusanzeige nicht mehr angezeigt und es wird weder eine Fehlermeldung noch eine Erfolgsmeldung angezeigt. Bei diesem Verhalten handelt es sich um ein zeitweiliges Problem.

Ursache

Die Statusanzeige wird nicht mehr angezeigt, da einige Browser aufhören, auf eine Antwort vom Server zu warten. Der Clusterbeitrittsvorgang wird durch dieses Verhalten nicht beendet. Mithilfe der Protokolldatei unter `/var/log/vmware/vcac/vcac-config.log` können Sie überprüfen, ob der Clusterbeitrittsvorgang erfolgreich war.

Die Upgrade-Zusammenführung der PostgreSQL-Datenbank ist nicht erfolgreich

Die Zusammenführung der externen PostgreSQL-Datenbank mit der eingebetteten PostgreSQL-Datenbank war nicht erfolgreich.

Problem

Wenn die Upgrade-Zusammenführung der PostgreSQL-Datenbank nicht erfolgreich war, können Sie eine manuelle Zusammenführung vornehmen.

Lösung

- 1 Setzen Sie die virtuelle vRealize Automation-Appliance auf den Snapshot zurück, den Sie vor dem Upgrade erstellt haben.
- 2 Melden Sie sich bei der virtuellen vRealize Automation-Appliance an und führen Sie diesen Befehl aus, damit das Upgrade abgeschlossen werden kann, wenn die Datenbankzusammenführung nicht erfolgreich war.

```
touch /tmp/allow-external-db
```

Die automatische Zusammenführung wird durch den Befehl nicht deaktiviert.

- 3 Stellen Sie auf dem Remotehost mit der PostgreSQL-Datenbank mit dem psql-Tool eine Verbindung zur PostgreSQL-Datenbank her und führen Sie die folgenden Befehle aus.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-osspl";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

Der Benutzer in diesem Befehl ist „vcac“. Wenn vRealize Automation mit einem anderen Benutzer eine Verbindung zu der externen Datenbank herstellt, ersetzen Sie in diesem Befehl „vcac“ durch den Namen dieses Benutzers.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

- 4 Führen Sie das Upgrade aus.

Wenn das Upgrade erfolgreich ist, arbeitet das System wie erwartet mit der externen PostgreSQL-Datenbank. Stellen Sie sicher, dass die externe PostgreSQL-Datenbank ordnungsgemäß arbeitet.

- 5 Melden Sie sich bei der virtuellen vRealize Automation-Appliance an und führen Sie die folgenden Befehle aus.

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

Update der Replikat- vRealize Automation -Appliance schlägt fehl

Das Update der Replikat-vRealize Automation-Appliance schlägt während des Updates der Master-Appliance fehl.

Ursache

Ein Update einer Replikat-Appliance kann aufgrund von Konnektivitätsproblemen oder anderen Fehlern fehlschlagen. Wenn dies passiert, erhalten Sie eine Warnmeldung auf der Registerkarte **Update** der Master-vRealize Automation-Appliance, in der der fehlgeschlagene Replikatknoten markiert ist.

Lösung

- 1 Setzen Sie das System mithilfe eines Snapshots oder einer Sicherung der virtuellen Replikat-Appliance zurück und schalten Sie die Appliance ein.
- 2 Melden Sie sich bei der Verwaltungsschnittstelle der Replikat-vRealize Automation-Appliance als Root-Benutzer an.

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

- 3 Klicken Sie auf **Update > Einstellungen**.

- 4 Geben Sie im Abschnitt „Update-Repository“ an, ob die Updates aus einem VMware-Repository oder von einer CD-ROM heruntergeladen werden sollen.
- 5 Klicken Sie auf **Status**.
- 6 Klicken Sie auf **Nach Updates suchen**, um zu überprüfen, ob ein Update verfügbar ist.
- 7 Klicken Sie auf **Updates installieren**.
- 8 Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die besagt, dass das Update ausgeführt wird.

- 9 Öffnen Sie die Protokolldateien, um sich zu vergewissern, dass die Aktualisierung erfolgreich verläuft.
 - `/opt/vmware/var/log/vami/vami.log`
 - `/var/log/vmware/horizon/horizon.log`

Wenn Sie sich während des Upgrade-Prozesses abmelden und anschließend wieder anmelden, bevor das Upgrade abgeschlossen ist, wird der Fortschritt des Updates in der Protokolldatei angezeigt. In der Datei `updatecli.log` werden möglicherweise Informationen zu der Version von vRealize Automation angezeigt, für die Sie das Upgrade durchführen. Diese angezeigte Version wird später im Upgrade-Vorgang in die entsprechende Version geändert.

Die benötigte Zeit für das Abschließen des Updates hängt von Ihrer Umgebung ab.

- 10 Starten Sie nach der Installation des Updates die virtuelle Appliance.
 - a Klicken Sie auf **System**.
 - b Klicken Sie auf **Neustart** und bestätigen Sie Ihre Auswahl.

- 11 Wählen Sie **vRA-Einstellungen > Cluster** aus.

- 12 Geben Sie den FQDN der Master-vRealize Automation-Appliance ein und klicken Sie auf **Cluster beitreten**.

Sicherungskopien von XML-Dateien führen zu einer Zeitüberschreitung des Systems

vRealize Automation registriert alle Dateien mit der Erweiterung „.xml“ im Verzeichnis „\VMware\CAC\Server\ExternalWorkflows\xml\“. Wenn dieses Verzeichnis Sicherungsdateien mit der Erweiterung „.xml“ enthält, führt das System doppelte Workflows aus, die zu einer Zeitüberschreitung des Systems führen.

Lösung

Problemumgehung: Wenn Sie Dateien in diesem Verzeichnis sichern, verschieben Sie die Sicherungskopien in ein anderes Verzeichnis oder ändern Sie den Dateierweiterungsnamen der Sicherungsdatei in eine andere Erweiterung als „.xml“.

Ausschließen des IaaS-Upgrades

Sie können die vRealize Automation-Appliance ohne Upgrade der IaaS-Komponenten aktualisieren.

Befolgen Sie diese Schritte, wenn Sie die vRealize Automation-Appliance ohne Upgrade der IaaS-Komponenten aktualisieren möchten. Dieses Verfahren

- Beendet die IaaS-Dienste nicht.
- Überspringt die Aktualisierung der Verwaltungs-Agents.
- Verhindert die automatische Aktualisierung der IaaS-Komponenten nach dem Update der vRealize Automation-Appliance.

Verfahren

- 1 Öffnen Sie eine Secure Shell-Verbindung zum Knoten der primären vRealize Automation-Appliance.
- 2 Führen Sie in der Eingabeaufforderung diesen Befehl aus, um die Toggle-Datei zu erstellen:
touch /tmp/disable-iaas-upgrade
- 3 Halten Sie die IaaS-Dienste manuell an.
 - a Melden Sie sich bei Ihrem IaaS-Windows-Server an.
 - b Wählen Sie **Start > Verwaltung > Dienste** aus.
 - c Halten Sie diese Dienste in der folgenden Reihenfolge an.

Hinweis Fahren Sie den IaaS-Windows-Server nicht herunter.

- 1 Jeder VMware vRealize Automation-Proxy-Agent.
 - 2 Jeder VMware-DEM-Worker.
 - 3 Der VMware-DEM-Orchestrator.
 - 4 Der VMware vCloud Automation Center-Dienst.
- 4 Greifen Sie auf die Verwaltungskonsole der primären vRealize Automation-Appliance zu und aktualisieren Sie die primäre vRealize Automation-Appliance.

Es kann kein neues Verzeichnis in vRealize Automation erstellt werden

Der Versuch, dem ersten Sync-Konnektor ein neues Verzeichnis hinzuzufügen, schlägt fehl.

Problem

Dieses Problem tritt aufgrund einer fehlerhaften Datei `config-state.json` im Verzeichnis `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/` auf.

Weitere Informationen zum Beheben dieses Problems finden Sie im [Knowledgebase-Artikel 2145438](#).

Zeitüberschreitung beim Update der virtuellen Replikate- vRealize Automation -Appliance

Das Update der virtuellen Replikate-vRealize Automation-Appliance wird wegen Zeitüberschreitung abgebrochen, wenn Sie die virtuelle Master-Appliance aktualisieren.

Problem

Wenn Sie die virtuelle Master-Appliance aktualisieren, wird auf der Registerkarte für die Verwaltungskontrolle der Master-vRealize Automation-Appliance eine markierte virtuelle Replikat-Appliance angezeigt, die den Zeitüberschreitungsgrenzwert für das Update überschritten hat.

Ursache

Die Zeit für das Update wurde aufgrund eines Leistungs- oder Infrastrukturproblems überschritten.

Lösung

- 1 Überprüfen Sie den Fortschritt des Updates der virtuellen Replikat-Appliance.
 - a Wechseln Sie zur Verwaltungskontrolle für Ihre virtuelle Replikat-Appliance unter Verwendung des vollqualifizierten Domännennamens (FQDN) „`https://va-hostname.domain.name:5480`“.
 - b Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance eingegeben haben.
 - c Wählen Sie **Aktualisieren > Status** aus und überprüfen Sie den Fortschritt des Updates.

Führen Sie einen der folgenden Schritte aus.

 - Wenn die Aktualisierung fehlschlägt, führen Sie die Schritte im Thema zur Fehlerbehebung [Update der Replikat-vRealize Automation-Appliance schlägt fehl](#) aus.
 - Wenn das Upgrade der virtuellen Replikat-Appliance ausgeführt wird, warten Sie, bis das Upgrade abgeschlossen ist und fahren Sie mit Schritt 2 fort.
- 2 Starten Sie die virtuelle Appliance neu.
 - a Klicken Sie auf **System**.
 - b Klicken Sie auf **Neustart** und bestätigen Sie Ihre Auswahl.
- 3 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 4 Geben Sie den FQDN der virtuellen Master-vRealize Automation-Appliance ein und klicken Sie auf **Cluster beitreten**.

Für einige virtuelle Maschinen wird während des Upgrades keine Bereitstellung erstellt

Virtuelle Maschinen, die zum Zeitpunkt des Upgrades den Status „Fehlt“ aufweisen, verfügen nicht über eine entsprechende in der Zielumgebung erstellte Bereitstellung.

Problem

Wenn eine virtuelle Maschine in der Quellumgebung während des Upgrades den Status „Fehlt“ aufweist, wird in der Zielumgebung keine entsprechende Bereitstellung erstellt. Wenn eine virtuelle Maschine nach dem Upgrade den Status „Fehlt“ verlässt, können Sie die Maschine unter Verwendung der Massenimportfunktion in die Zielumgebung importieren.

Fehler „Zertifikat nicht vertrauenswürdig“

Wenn Sie die Seite „Protokoll-Viewer“ in der vRealize Automation-Appliance-Konsole öffnen, wird möglicherweise ein Fehlerbericht für eine Endpoint-Verbindung mit diesen Worten angezeigt: `Certificate is not trusted`.

Problem

Wählen Sie auf der vRealize Automation-Appliance-Konsole **Infrastruktur > Überwachung > Protokoll** aus. Auf der Seite „Protokoll-Viewer“ wird möglicherweise ein Bericht ähnlich dem Folgenden angezeigt:

Failed to connect to the endpoint. To validate that a secure connection can be established to this endpoint, go to the vSphere endpoint on the Endpoints page and click the Test Connection button.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.my-company.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Ursache

Das Upgrade von vRealize Automation 7.3 oder früher auf 7.4 nimmt Änderungen an den Endpoints der ursprünglichen Umgebung vor. In Umgebungen, die kürzlich auf vRealize Automation 7.4 aktualisiert wurden, muss der IaaS-Administrator jeden vorhandenen Endpoint überprüfen, der eine sichere HTTPS-Verbindung verwendet. Wenn für einen Endpoint der Fehler `Certificate is not trusted` angezeigt wird, funktioniert der Endpoint nicht ordnungsgemäß.

Lösung

- 1 Melden Sie sich bei der vRealize Automation-Konsole als Infrastrukturadministrator an.
- 2 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 3 Führen Sie diese Schritte für jeden Endpoint mit einer sicheren Verbindung durch.
 - a Klicken Sie auf **Bearbeiten**.
 - b Klicken Sie auf **Testverbindung**.
 - c Überprüfen Sie die Zertifikatdetails und klicken Sie auf **OK**, wenn Sie das Zertifikat als vertrauenswürdig einstufen.
 - d Starten Sie die Windows-Dienste für alle IaaS-Proxy-Agents, die von diesem Endpoint verwendet werden.
- 4 Stellen Sie sicher, dass keine Fehler `Certificate is not trusted` auf der Seite „Protokoll-Viewer“ mehr angezeigt werden.

Installation von oder Upgrade auf vRealize Automation schlägt fehl

Die Installation oder das Upgrade von vRealize Automation schlägt fehl, und in der Protokolldatei wird eine Fehlermeldung angezeigt.

Problem

Wenn Sie vRealize Automation installieren oder ein Upgrade dazu durchführen, schlägt der Vorgang fehl. Dies geschieht in der Regel, wenn ein Fix, der während der Installation oder des Upgrades angewendet wird, nicht erfolgreich ist. In der Protokolldatei wird eine Fehlermeldung ähnlich der folgenden angezeigt: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Ursache

Die Windows-Umgebung hat eine Gruppenrichtlinie für die Ausführung von PowerShell-Skripten auf „Aktiviert“ gesetzt.

Lösung

- 1 Führen Sie auf der Windows-Hostmaschine `gpedit.msc` aus, um den lokalen Gruppenrichtlinien-Editor zu öffnen.
- 2 Klicken Sie im linken Bereich unter **Computerkonfiguration** auf die Schaltfläche zum Erweitern, um **Administrative Vorlagen > Windows-Komponenten > Windows PowerShell** zu öffnen.
- 3 Ändern Sie die Einstellung von **Skriptausführung aktivieren** von **Enabled** in **Not Configured**.

Aktualisieren von DEM- und DEO-Komponenten nicht möglich

Aktualisieren von DEM- und DEO-Komponenten beim Upgrade von vRealize Automation 7.2 auf 7.3.x nicht möglich

Problem

Nach dem Aktualisieren von vRealize Automation 7.2 auf 7.3.x werden in einem benutzerdefinierten Pfad, wie beispielsweise auf dem Laufwerk D:, installierte DEM- und DEO-Komponenten nicht aktualisiert.

Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2150517](#).

Beim Update wird kein Upgrade des Management Agents durchgeführt

Eine Fehlermeldung bezüglich des Verwaltungsagenten wird angezeigt, wenn Sie auf der Seite „Status aktualisieren“ der vRealize Automation-Appliance-Verwaltungskonsole auf **Updates installieren** klicken.

Problem

Upgrade-Prozess ist fehlgeschlagen. Folgende Fehlermeldung wird angezeigt: Management-Agent auf Knoten x konnte nicht aktualisiert werden. In manchen Fällen werden in dieser Meldung mehrere Knoten aufgelistet.

Ursache

Für dieses Problem gibt es zahlreiche Ursachen. In der Fehlermeldung wird nur die Knoten-ID der betroffenen Maschine angegeben. Weitere Informationen finden Sie in der Datei `ALL.log` für den Management-Agent auf der Maschine, auf der der Befehl fehlgeschlagen ist.

Führen Sie diese Aufgaben entsprechend der bei Ihnen vorliegenden Situation auf den betroffenen Knoten durch:

Lösung

- Wenn der Management-Agent-Dienst nicht ausgeführt wird, starten Sie den Dienst und starten Sie das Upgrade auf der virtuellen Appliance neu.
- Wenn der Management-Agent-Dienst ausgeführt wird und ein Upgrade des Management-Agents durchgeführt wird, starten Sie das Upgrade auf der virtuellen Appliance neu.
- Wenn der Management-Agent-Dienst ausgeführt wird, jedoch kein Upgrade des Management-Agents durchgeführt wird, führen Sie ein manuelles Upgrade durch.
 - a Öffnen Sie einen Browser und wechseln Sie zur Seite „vRealize Automation-aaS-Installation“ auf der vRealize Automation-Appliance unter `https:// va-hostname.domain.name:5480/in-stall`.
 - b Laden Sie das Installationsprogramm für den Management-Agent herunter und führen Sie es aus.
 - c Starten Sie die Management-Agent-Maschine neu.
 - d Starten Sie das Upgrade auf der virtuellen Appliance neu.

Upgrade des Management-Agents war nicht erfolgreich

Beim Upgrade von vRealize Automation auf 7.2 bis 7.3.x ist das Upgrade des Management Agents nicht erfolgreich.

Problem

Wenn bei einem Failover-Vorfall ein Wechsel zwischen dem primären und dem sekundären Management-Agent-Host stattgefunden hat, ist das Upgrade nicht erfolgreich, weil der erwartete Host beim automatisierten Upgrade-Vorgang nicht gefunden wird. Führen Sie dieses Verfahren auf jedemaaS-Knoten durch, auf dem der Management-Agent nicht aktualisiert wurde.

Lösung

- 1 Öffnen Sie die Datei „All.log“ im Protokollordner des Management-Agents unter `C:\Programme (x86)\VMware\VCAC\Management Agent\Logs\`.

Der Speicherort des Installationsordners kann vom Standardspeicherort abweichen.

- 2 Durchsuchen Sie die Protokolldatei nach einer Meldung über eine veraltete oder ausgeschaltete virtuelle Appliance.

Beispiel: INNERE AUSNAHME: System.Net.WebException: Verbindung zum Remoteserver nicht möglich ---> System.Net.Sockets.SocketException: Ein Verbindungsversuch ist fehlgeschlagen, da die verbundene Partei nach einem bestimmten Zeitraum nicht ordnungsgemäß geantwortet hat, oder die eingerichtete Verbindung ist ausgefallen, da der verbundene Host nicht geantwortet hat `IP_Address:5480`

- 3 Bearbeiten Sie die Konfigurationsdatei des Management-Agents unter C:\Programme (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config und ersetzen Sie den vorhandenen Wert „alternativeEndpointaddress“ durch die URL des Endpoints der primären virtuellen Appliance.

Der Speicherort des Installationsordners kann vom Standardspeicherort abweichen.

Beispiel für „alternativeEndpointaddress“ in VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 Starten Sie den Management-Agent-Windows-Dienst neu und überprüfen Sie anhand der Datei All.log, ob er arbeitet.
- 5 Führen Sie das Upgrade-Verfahren auf der primären vRealize Automation-Appliance durch.

Update von vRealize Automation schlägt aufgrund von Standardeinstellungen für die Zeitüberschreitung fehl

Sie können die Zeiteinstellung für Updates erhöhen, wenn die Standardeinstellung für die Synchronisierung von Datenbanken für Ihre Umgebung zu kurz ist.

Problem

Der Zeitüberschreitungswert für den Vcac-Config-Befehl SynchronizeDatabases reicht für bestimmte Umgebungen nicht aus, in denen die Synchronisierung von Datenbanken länger als der Standardwert von 3600 Sekunden dauert.

Die Eigenschaftswerte cafeTimeoutInSeconds und cafeRequestPageSize in der Datei Vcac-Config.exe.config steuern die Kommunikation zwischen der API und dem Vcac-config.exe-Hilfsprogramm. Die Datei befindet sich im Speicherort der IaaS-Installation\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config.

Sie können den standardmäßigen Zeitüberschreitungswert ausschließlich für den Befehl SynchronizeDatabases überschreiben, indem Sie einen Wert für diese optionalen Parameter angeben.

Parameter	Kurzname	Beschreibung
--DatabaseSyncTimeout	-dstm	Legt den Zeitüberschreitungswert der HTTP-Anforderung ausschließlich für SynchronizeDatabases in Sekunden fest.
--DatabaseSyncPageSize	-dsps	Legt die Seitengröße der Synchronisierungsanforderung ausschließlich für die Synchronisierung von Reservierungen oder Reservierungsrichtlinien fest. Die Standardeinstellung ist 10.

Wenn diese Parameter in der Datei Vcac-Config.exe.config nicht festgelegt sind, verwendet das System den standardmäßigen Zeitüberschreitungswert.

Fehlschlagen des Upgrades von IaaS in einer Hochverfügbarkeitsumgebung

Die Ausführung des IaaS-Upgrades auf einem primären Webserverknoten mit aktiviertem Lastausgleich schlägt fehl. Möglicherweise werden diese Fehlermeldungen angezeigt: "System.Net.WebException: Der Vorgang wurde wegen Zeitüberschreitung abgebrochen" oder "401 - Nicht autorisiert: Zugriff wurde aufgrund von falschen Anmeldedaten verweigert."

Problem

Ein Upgrade von IaaS mit aktiviertem Lastausgleich kann einen vorübergehenden Fehler verursachen. Wenn dieser Fall eintritt, müssen Sie das vRealize Automation-Upgrade erneut mit deaktiviertem Lastausgleich ausführen.

Lösung

- 1 Setzen Sie Ihre Umgebung auf die Snapshots vor dem Upgrade zurück.
- 2 Öffnen Sie eine Remotedesktopverbindung auf dem primären IaaS-Webserver-Knoten.
- 3 Navigieren Sie zur Windows-Host-Datei (c:\windows\system32\drivers\etc).
- 4 Öffnen Sie die Host-Datei und fügen Sie die folgende Zeile hinzu, um den Webserver-Lastausgleich zu umgehen.

```
IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn
```

Beispiel:

```
10.10.10.5 vra-iaas-web-lb.domain.com
```

- 5 Speichern Sie die Host-Datei und führen Sie das vRealize Automation-Upgrade erneut aus.
- 6 Wenn das vRealize Automation-Update abgeschlossen ist, öffnen Sie die Host-Datei und entfernen Sie die Zeile, die Sie in Schritt 4 hinzugefügt haben.

Umgehen von Problemen beim Upgrade

Sie können den Upgradevorgang anpassen, um Probleme beim Upgrade zu umgehen.

Lösung

Wenn beim Upgrade Ihrer vRealize Automation-Umgebung Probleme auftreten, verwenden Sie das folgende Verfahren, um den Upgradevorgang durch Auswahl eines der verfügbaren Flags zu ändern.

Verfahren

- 1 Öffnen Sie eine Secure Shell-Verbindung zum Knoten der primären vRealize Automation-Appliance.

2 Führen Sie in der Eingabeaufforderung diesen Befehl aus, um die Toggle-Datei zu erstellen:

touch available_flag

Beispiel: **touch /tmp/disable-iaas-upgrade**

Tabelle 1-60. Verfügbare Flags

Flag	Beschreibung
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Verhindert das IaaS-Upgrade nach dem Neustart der virtuellen Appliance. ■ Verhindert das Upgrade des Management-Agent. ■ Verhindert die automatische Überprüfung der Voraussetzungen und etwaige Fehlerbehebungen. ■ Verhindert das Beenden von IaaS-Diensten.
/tmp/do-not-upgrade-ma	Verhindert das Upgrade des Management-Agent. Dieses Flag ist geeignet, wenn der Management-Agent manuell aktualisiert wird.
/tmp/skip-prereq-checks	Verhindert die automatische Überprüfung der Voraussetzungen und etwaige Fehlerbehebungen. Dieses Flag ist geeignet, wenn ein Problem bei der automatischen Fehlerbehebung der Voraussetzungen auftritt und die Fehlerbehebung stattdessen manuell durchgeführt werden.
/tmp/do-not-stop-services	Verhindert das Beenden von IaaS-Diensten. Das Upgrade hält die IaaS-Windows-Dienste, wie z. B. den Manager Service, DEM-Instanzen und Agents, nicht an.
/tmp/do-not-upgrade-servers	<p>Verhindert das automatische Upgrade aller IaaS-Serverkomponenten, wie die Datenbank, Website, WAPI, Repository, Model Manager-Daten und Manager Service.</p> <p>Hinweis Dieses Flag verhindert zudem die Aktivierung des automatischen Manager Service-Failover-Modus.</p>
/tmp/do-not-upgrade-dems	Verhindert das DEM-Upgrade.
/tmp/do-not-upgrade-agents	Verhindert das Upgrade des IaaS-Proxy-Agent.

3 Führen Sie die Aufgaben für Ihr ausgewähltes Flag durch.

Tabelle 1-61. Zusätzliche Aufgaben

Flag	Aufgaben
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Aktualisieren Sie den Management-Agent manuell. ■ Wenden Sie alle erforderlichen IaaS-Komponenten manuell an. ■ Halten Sie die IaaS-Dienste manuell an. <ol style="list-style-type: none"> a Melden Sie sich bei Ihrem IaaS-Windows-Server an. b Wählen Sie Start > Verwaltung > Dienste aus. c Halten Sie diese Dienste in der folgenden Reihenfolge an. <p>Hinweis Fahren Sie den IaaS-Windows-Server nicht herunter.</p> <ol style="list-style-type: none"> a Jeder VMware vRealize Automation-Proxy-Agent. b Jeder VMware-DEM-Worker. c Der VMware-DEM-Orchestrator. d Der VMware vCloud Automation Center-Dienst. ■ Starten Sie das IaaS-Upgrade manuell, nachdem das Upgrade der virtuellen Appliance abgeschlossen ist.
/tmp/do-not-upgrade-ma	Aktualisieren Sie den Management-Agent manuell.
/tmp/skip-prereq-checks	Wenden Sie alle erforderlichen IaaS-Komponenten manuell an.
/tmp/do-not-stop-services	<p>Halten Sie die IaaS-Dienste manuell an.</p> <ol style="list-style-type: none"> 1 Melden Sie sich bei Ihrem IaaS-Windows-Server an. 2 Wählen Sie Start > Verwaltung > Dienste aus. 3 Halten Sie diese Dienste in der folgenden Reihenfolge an. <p>Hinweis Fahren Sie den IaaS-Windows-Server nicht herunter.</p> <ol style="list-style-type: none"> a Jeder VMware vRealize Automation-Proxy-Agent. b Jeder VMware-DEM-Worker. c Der VMware-DEM-Orchestrator. d Der VMware vCloud Automation Center-Dienst.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 Greifen Sie auf die Verwaltungskonsole der primären vRealize Automation-Appliance zu und aktualisieren Sie die primäre vRealize Automation-Appliance.

Hinweis Da jedes Flag bis zu seinem Entfernen aktiv bleibt, führen Sie diesen Befehl aus, um Ihr ausgewähltes Flag nach dem Upgrade zu entfernen: `rm /flag_path/flag_name`. Beispiel: `rm /tmp/disable-iaas-upgrade`.

Upgrade von vRealize Automation 6.2.5 auf 7.4

Bei einem Upgrade Ihrer Umgebung mit vRealize Automation 6.2.5 auf die neueste Version verwenden Sie die Upgrade-Verfahren für Ihre Umgebung der Version 6.2.5.

Diese Informationen gelten für das Upgrade von vRealize Automation 6.2.5 auf 7.4. Informationen zu anderen unterstützten Upgrade-Pfaden finden Sie unter [Aktualisieren von vRealize Automation](#).

Upgrade von vRealize Automation 6.2.5 auf 7.4

Sie können ein direktes Upgrade Ihrer aktuellen vRealize Automation 6.2.5-Umgebung auf 7.4 durchführen. Für das Upgrade Ihrer Umgebung verwenden Sie die für diese Version spezifischen Upgrade-Verfahren.

Ein direktes Upgrade ist ein aus drei Stufen bestehendes Verfahren. Sie aktualisieren die Komponenten in Ihrer aktuellen Umgebung in dieser Reihenfolge.

- 1 vRealize Automation-Appliance
- 2 IaaS-Webserver
- 3 vRealize Orchestrator

Sie müssen bei allen Produktkomponenten ein Upgrade auf dieselbe Version durchführen.

Das vRealize Production Test Upgrade Assist-Tool analysiert Ihre vRealize Automation 6.2.x-Umgebung hinsichtlich jeder Funktionskonfiguration, die Upgrade-Probleme verursachen kann, und überprüft, ob Ihre Umgebung für das Upgrade bereit ist. Um dieses Tool und die zugehörige Dokumentation herunterzuladen, navigieren Sie zur Downloadseite für das [VMware vRealize Production Test Tool](#).

Steuerelemente von Eigenschaftswörterbüchern, die nach dem Upgrade nicht unterstützt werden, können mithilfe von vRealize Orchestrator und Beziehungen von Eigenschaftswörterbüchern wiederhergestellt werden.

Wenn Ihre Quellumgebung Workflows mit veraltetem Code enthält, erhalten Sie Informationen zu Codeänderungen, die für die Umwandlung in Ereignisbrokerabonnements notwendig sind, im [vRealize Automation Extensibility Migration Guide](#).

Ab vRealize Automation 7.2 wird JFrog Artifactory Pro nicht mehr im Paket mit der vRealize Automation-Appliance-Appliance angeboten. Wenn Sie ein Upgrade von einer früheren Version von vRealize Automation durchführen, wird JFrog Artifactory Pro während des Upgradevorgangs entfernt. Weitere Informationen finden Sie im [Knowledgebase-Artikel 2147237](#).

Hinweis Falls Sie Ihre aktuelle vRealize Automation 6.2.5-Umgebung angepasst haben, wenden Sie sich wegen zusätzlicher Upgradeinformationen an die Mitarbeiter des CCE-Supports.

Voraussetzungen für das Aktualisieren von vRealize Automation

Überprüfen Sie vor dem Upgrade von vRealize Automation 6.2.5 die folgenden Voraussetzungen.

Systemkonfigurationsanforderungen

Vergewissern Sie sich vor dem Beginn einer Aktualisierung, dass die folgenden Systemanforderungen erfüllt sind.

- Stellen Sie sicher, dass alle Appliances und Server, die Teil der Bereitstellung sind, die Systemanforderungen für die neueste Version erfüllen. Weitere Informationen finden Sie unter *vRealize AutomationSupport-Matrix* in der [VMware vRealize Automation-Dokumentation](#).
- In der *VMware Product Interoperability Matrix* auf der VMware-Website finden Sie Informationen über die Kompatibilität mit anderen VMware-Produkten.
- Stellen Sie sicher, dass es sich bei der vRealize Automation-Version, von der aus Sie das Upgrade durchführen, um eine stabile Version handelt. Korrigieren Sie etwaige Probleme vor der Durchführung des Upgrades.
- Wenn Sie von vRealize Automation 6.2.5 aktualisieren, notieren Sie den vCloud Suite-Lizenzschlüssel für Ihre aktuelle vRealize Automation-Umgebung. Beim Upgrade werden vorhandene Lizenzschlüssel aus der Datenbank entfernt.
- Vergewissern Sie sich, dass Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst vom Standardwert auf mindestens 10 Minuten geändert haben.

Hardwarekonfigurationsanforderungen

Vergewissern Sie sich, dass die Hardware in Ihrer Umgebung für Ihre vRealize Automation-Zielversion geeignet ist.

Siehe [vRealize Automation-Hardware-Spezifikationen und maximale Kapazitäten](#).

Vergewissern Sie sich vor dem Beginn einer Aktualisierung, dass die folgenden Systemanforderungen erfüllt sind.

- Sie müssen Ihre aktuelle Hardware konfigurieren, bevor Sie das Upgrade herunterladen. Siehe [Erweitern der vCenter Server-Hardwareressourcen für vRealize Automation 6.2.5](#).
- Sie müssen mindestens über 18 GB RAM, 4 CPUs, Disk1 = 50 GB, Disk3=25 GB und Disk4=50 GB verfügen, bevor Sie das Upgrade ausführen können.

Wenn die virtuelle Maschine unter vCloud Networking and Security ausgeführt wird, müssen Sie möglicherweise mehr RAM-Speicher zuteilen.

Obwohl die allgemeine Unterstützung für vCloud Networking and Security beendet wurde, sind die benutzerdefinierten VCNS-Eigenschaften nach wie vor zu NSX-Zwecken gültig. Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2144733](#).

- Die folgenden Knoten müssen mindestens über 5 GB freien Festplattenspeicher verfügen:
 - Primäre IaaS-Website
 - Microsoft SQL-Datenbank
 - Model Manager
- Der primäre IaaS-Websiteknoten, auf dem die Model Manager-Daten installiert sind, muss über JAVA SE Runtime Environment 8, 64 Bit, Update 161 oder höher verfügen. Nach der Installation von Java müssen Sie die Umgebungsvariable JAVA_HOME auf die neue Version aktualisieren.
- Um das Upgrade herunterzuladen und auszuführen, benötigen Sie die folgenden Ressourcen:
 - Mindestens 5 GB auf der Root-Partition
 - 5 GB auf der Partition /storage/db für die Master-vRealize Automation-Appliance
 - 5 GB auf der Root-Partition für jede virtuelle Replikat-Appliance
- Öffnen Sie den Unterordner /storage/log und entfernen Sie alle älteren archivierten ZIP-Dateien, um Speicherplatz zu bereinigen.

Allgemeine Voraussetzungen

Vergewissern Sie sich vor dem Beginn einer Aktualisierung, dass die folgenden Systemanforderungen erfüllt sind.

- Sie haben Zugriff auf ein Active Directory-Konto im Format Benutzername@Domäne und Berechtigungen zum Binden an das Verzeichnis.
- Diese Bedingungen sind erfüllt:
 - Sie haben Zugriff auf ein Konto mit einem SAMaccountName-Format.
 - Sie verfügen über die erforderlichen Rechte, um das System mit der Domäne zu verbinden, indem Sie dynamisch ein Computerobjekt erstellen, oder um es mit einem zuvor erstellten Objekt zusammenzuführen.
- Sie haben Zugriff auf alle Datenbanken und alle Lastausgleichsdienste, die von dem Upgrade für vRealize Automation betroffen sind oder daran beteiligt sind.
- Während der Durchführung des Upgrades ist das System für Benutzer nicht verfügbar.
- Sie deaktivieren alle Anwendungen, die vRealize Automation abfragen.
- Stellen Sie sicher, Microsoft Distributed Transaction Coordinator (MSDTC) auf allen vRealize Automation- und zugehörigen SQL-Servern aktiviert ist. Weitere Anweisungen finden Sie im [Knowledgebase-Artikel 2089503](#).

- Wenn Ihre Umgebung über eine externe vRealize Orchestrator-Appliance verfügt und eine externe vRealize Orchestrator-Appliance mit der Identity Appliance verbunden ist, aktualisieren Sie vRealize Orchestrator vor dem Upgrade von vRealize Automation.
- Sie müssen zusätzliche Aufgaben ausführen, um Ihre virtuellen vRealize Automation-Maschinen vor dem Upgrade vorzubereiten. Lesen Sie vor dem Upgrade den [Knowledgebase-Artikel 51531](#).
- Vergewissern Sie sich, dass Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst vom Standardwert auf mindestens 10 Minuten geändert haben.
- Wenn Sie das DynamicTypes-Plug-In verwenden, müssen Sie die DynamicTypes-Plug-In-Konfigurationen von vRealize Orchestrator als Paketworkflow exportieren.

`/Library/Dynamic Types/Configuration/Export Configuration As Package`

- Führen Sie diese Schritte aus, wenn Sie eine verteilte Umgebung aktualisieren, die mit einer eingebetteten PostgreSQL-Datenbank konfiguriert wurde.
 - a Überprüfen Sie die Dateien im Verzeichnis `pgdata` auf dem Master-Host, bevor Sie die Replikat-Hosts aktualisieren.
 - b Navigieren Sie zum PostgreSQL-Datenordner auf dem Master-Host unter `/var/vmware/vpostgres/current/pgdata/`.
 - c Schließen Sie alle geöffneten Dateien im Verzeichnis `pgdata` und entfernen Sie alle Dateien mit dem Suffix „.swp“.
 - d Stellen Sie sicher, dass alle Dateien in diesem Verzeichnis über den richtigen Besitzer verfügen: `postgres:users`.

Überlegungen zum Upgrade auf diese vRealize Automation -Version

vRealize Automation 7 und höher führt während und nach dem Upgrade-Vorgang verschiedene funktionale Änderungen ein. Sie sollten Änderungen überprüfen, bevor Sie ein Upgrade Ihrer vRealize Automation 6.2.5-Bereitstellung auf die neue Version durchführen.

Prüfen Sie diese Überlegungen, bevor Sie ein Upgrade durchführen.

Aktualisierung und Identity Appliance-Spezifikationen

Während des Aktualisierungsvorgangs von vRealize Automation beachten Sie die Eingabeaufforderungen, um die Identity Appliance zu aktualisieren.

Die Zielbereitstellung verwendet den VMware Identity Manager.

Aktualisierung und Lizenzierung

Während der Aktualisierung werden Ihre vorhandenen vRealize Automation 6.2.5-Lizenzen und alle vCloud Suite 6.x-Lizenzen entfernt. Sie müssen die Lizenzen in der Verwaltungskonsole der vRealize Automation 7.4-Appliance erneut eingeben. vRealize Automation

Nun verwenden Sie die vRealize Automation-Lizenzierung für virtuelle Appliances und IaaS, indem Sie Lizenzschlüsselinformationen in der vRealize Automation-Appliance eingeben. Lizenzierungsinformationen sind in der IaaS-Benutzeroberfläche nicht mehr verfügbar und IaaS prüft die Lizenzen nicht mehr. Endpoints und Kontingente werden über Endbenutzer-Lizenzvereinbarungen (EULAs) durchgesetzt.

Hinweis Notieren Sie sich vor dem Upgrade den Lizenzschlüssel von vCloud Suite 6.x, falls Sie ihn für vRealize Automation 6.2.5 verwendet haben. Beim Upgrade werden vorhandene Lizenzschlüssel aus der Datenbank entfernt.

Weitere Informationen zum erneuten Eingeben Ihrer Lizenzinformationen während oder nach einem Upgrade finden Sie unter [Aktualisieren des Lizenzschlüssels](#).

Grundlegendes zum Aktualisieren von Rollen

Wenn Sie vRealize Automation aktualisieren, werden die vorhandenen Rollenzuweisungen der Organisation beibehalten. Durch die Aktualisierung werden auch einige Rollenzuweisungen zum Unterstützen von zusätzlichen Blueprint-Architekt-Rollen erstellt.

Die folgenden Architekt-Rollen werden zum Unterstützen der Blueprint-Definition in der Design-Arbeitsfläche verwendet:

- Anwendungsarchitekt: stellt vorhandene Komponenten und Blueprints zum Erstellen von zusammengesetzten Blueprints zusammen
- Infrastrukturarchitekt. Erstellt und verwaltet Blueprints der virtuellen Maschine.
- XaaS-Architekt Erstellt und veröffentlicht von XaaS-Blueprints
- Softwarearchitekt: erstellt und verwaltet Software-Komponenten

Mandantenadministratoren und Business-Gruppenmanager können in vRealize Automation 7 Blueprints nicht standardmäßig entwerfen. Aktualisierte Mandantenadministratoren und Business-Gruppenmanager erhalten die Rolle „Infrastrukturarchitekt“.

Benutzer, die eine virtuelle Maschine in der Quellversion vRealize Automation 6.2.x neu konfigurieren können, können den Besitzer der virtuellen Maschine ändern, nachdem sie ein Upgrade auf die neue Version durchgeführt haben.

Die folgenden Rollenzuweisungen werden bei der Aktualisierung vorgenommen. Nicht in der Tabelle aufgeführte Rollen werden auf die Rolle mit demselben Namen in der Zielbereitstellung aktualisiert.

Tabelle 1-62. Während des Upgrades zugewiesene Rollen

Rolle in der Quellbereitstellung	Rolle in der Zielbereitstellung
Mandantenadministrator	Mandantenadministrator und Infrastrukturarchitekt
Business-Gruppenmanager	Business-Gruppenmanager und Infrastrukturarchitekt
Dienstarchitekt	XaaS-Architekt
Anwendungsarchitekt	Softwarearchitekt

Weitere Informationen zu Rollen finden Sie unter [Mandantenrollen und -aufgaben in vRealize Automation](#).

Grundlegendes zum Aktualisieren von Blueprints

In der Regel werden veröffentlichte Blueprints als veröffentlichte Blueprints aktualisiert.

Es gibt jedoch Ausnahmen von dieser Regel. Multi-Maschinen-Blueprints werden als zusammengesetzte Blueprints aktualisiert, die Blueprint-Komponenten enthalten. Multi-Maschinen-Blueprints, die nicht unterstützte Einstellungen enthalten, werden als nicht veröffentlicht aktualisiert.

Hinweis vRealize Automation 7.x erstellt bei der Bereitstellung einen Blueprint-Snapshot. Falls Sie bei einer Bereitstellung auf Neukonfigurationsprobleme bei der Aktualisierung von Maschineneigenschaften wie z. B. CPU und RAM stoßen, lesen Sie den Knowledgebase-Artikel [2150829 vRA 7.x Blueprint Snapping](#).

Weitere Informationen zum Upgrade von Blueprints finden Sie unter [Upgrade und vApp-Blueprints](#), [vCloud-Endpoints und vCloud-Reservierungen](#) und [Grundlegendes zum Aktualisieren von Multi-Maschinen-Blueprints](#).

Upgrade und vApp-Blueprints, vCloud-Endpoints und vCloud-Reservierungen

Sie können keine Bereitstellung aktualisieren, die vApp (vCloud)-Endpoints enthält. vApp-Endpoints (vCloud) verhindern das Upgrade auf diese vRealize Automation-Version.

Das Upgrade auf der virtuellen Master-Appliance schlägt fehl, wenn es in der Quellbereitstellung einen vApp- (vCloud-)Endpoint gibt. Es wird eine Meldung in der Benutzeroberfläche und in der Protokolldatei angezeigt. Um festzustellen, ob Ihre Quellbereitstellung einen vApp-Endpoint (vCloud) enthält, melden Sie sich als IaaS-Administrator an der vRealize Automation-Konsole an. Wählen Sie **Infrastruktur > Endpoints** aus. Wenn die Liste der Endpoints vApp-Endpoints (vCloud) enthält, ist ein Upgrade auf die vRealize Automation-Version nicht möglich.

Verwaltete vApps für vCloud Air- oder vCloud Director-Ressourcen werden in der vRealize Automation-Zielumgebung nicht unterstützt.

Hinweis Die folgenden Arten von Genehmigungsrichtlinien sind veraltet. Wenn sie nach Abschluss des Upgrades in der Liste der verfügbaren Arten von Genehmigungsrichtlinien angezeigt werden, können sie nicht verwendet werden.

- Servicekatalog - Katalogelementanforderung - vApp
 - Servicekatalog - Katalogelementanforderung - vApp-Komponente
-

Sie können vCloud Air- und vCloud Director-Endpoints und -Reservierungen in der Zielbereitstellung erstellen. Zudem können Sie Blueprints mit virtuellen vCloud Air- oder vCloud Director-Maschinenkomponenten erstellen.

Grundlegendes zum Aktualisieren von Multi-Maschinen-Blueprints

Sie können verwaltete Multi-Maschinen-Dienst-Blueprints von einer unterstützten Bereitstellung der Version vRealize Automation 6.2.x aktualisieren.

Wenn Sie einen Multi-Maschinen-Blueprint aktualisieren, werden Komponenten-Blueprints als getrennte Einzelmaschinen-Blueprints aktualisiert. Der Multi-Maschinen-Blueprint wird als zusammengesetzter Blueprint aktualisiert, in dem die früheren untergeordneten Blueprints als getrennte Blueprint-Komponenten verschachtelt werden.

Das Upgrade erstellt einen einzelnen zusammengesetzten Blueprint in der Zielbereitstellung, der eine virtuelle Maschinenkomponente für jeden Komponenten-Blueprint im Multi-Maschinen-Quell-Blueprint enthält. Weist ein Blueprint eine Einstellung auf, die in der neuen Version nicht unterstützt wird, wird der Blueprint aktualisiert und erhält den Entwurfsstatus. Wenn beispielsweise der Multi-Maschinen-Blueprint ein privates Netzwerkprofil enthält, wird die Profileinstellung beim Upgrade ignoriert und der Blueprint wird in den Entwurfsstatus gesetzt. Sie können den Blueprint mit dem Status „Entwurf“ bearbeiten, um unterstützte Netzwerkprofilinformationen einzugeben und ihn zu veröffentlichen.

Hinweis Wenn ein veröffentlichter Blueprint in der Quellbereitstellung auf einen Blueprint mit dem Status „Entwurf“ aktualisiert wird, ist der Blueprint nicht mehr Teil eines Diensts oder einer Berechtigung. Nachdem Sie den Blueprint in der aktualisierten vRealize Automation-Version aktualisiert und veröffentlicht haben, müssen Sie die erforderlichen Genehmigungsrichtlinien und Berechtigungen erneut erstellen.

Manche Multi-Maschinen-Blueprint-Einstellungen werden in der vRealize Automation-Zielbereitstellung nicht unterstützt, darunter private Netzwerkprofile und geroutete Netzwerkprofile mit zugeordneten PLR-Edge-Einstellungen. Wenn Sie eine benutzerdefinierte Eigenschaft verwendet haben, um PLR-Edge-Einstellungen anzugeben (`VCNS.LoadBalancerEdgePool.Names`), wird die benutzerdefinierte Eigenschaft aktualisiert.

Sie können einen Multi-Maschinen-Blueprint mit vSphere-Endpoints und NSX-Netzwerk- und Sicherheitseinstellungen aktualisieren. Der aktualisierte Blueprint enthält NSX-Netzwerk- und Sicherheitskomponenten in der Design-Arbeitsfläche.

Hinweis Spezifikationen für geroutete Gateways für Multi-Maschinen-Blueprints, wie definiert in den Reservierungen, werden aktualisiert. Die vRealize Automation-Zielbereitstellung unterstützt jedoch keine Reservierungen für geroutete Profile, die zugeordnete PLR-Edge-Einstellungen enthalten. Wenn die Quellreservierung einen Wert eines gerouteten Gateways für einen PLR-Edge enthält, wird die Reservierung aktualisiert, die Einstellung für das geroutete Gateway wird jedoch ignoriert. Daher generiert die Aktualisierung eine Fehlermeldung in der Protokolldatei, und die Reservierung wird deaktiviert.

Während der Aktualisierung werden Leerzeichen und Sonderzeichen aus den referenzierten Netzwerk- und Sicherheitskomponentennamen entfernt.

Hinweis vRealize Automation 7.x erstellt bei der Bereitstellung einen Blueprint-Snapshot. Falls Sie bei einer Bereitstellung auf Neukonfigurationsprobleme bei der Aktualisierung von Maschineneigenschaften wie z. B. CPU und RAM stoßen, lesen Sie den Knowledgebase-Artikel [2150829 vRA 7.x Blueprint Snapping](#).

Je nach Einstellungstyp werden die Netzwerk- und Sicherheitsinformationen als mehrere unterschiedliche Einstellungen in dem neuen Blueprint erfasst.

- Einstellungen für den gesamten Blueprint auf seiner Eigenschaftenseite. Diese Informationen beinhalten Anwendungsisolierung, Transportzone und Reservierungsrichtlinieninformationen für geroutete Gateways oder NSX Edge.
- Verfügbare Einstellungen für virtuelle vSphere-Maschinenkomponenten in NSX-Netzwerk- und Sicherheitskomponenten in der Design-Arbeitsfläche.
- Einstellungen in den Registerkarten „Netzwerk“ und „Sicherheit“ der einzelnen virtuellen vSphere-Maschinenkomponenten in der Design-Arbeitsfläche.

Aktualisierung und physische Endpoints, Reservierungen und Blueprints

Sie können eine Bereitstellung nicht aktualisieren, die physische Endpoints enthält. Wenn physische Endpoints vorhanden sind, schlägt der vRealize Automation-Upgradevorgang fehl.

Wenn die vRealize Automation 6.2.x-Bereitstellung einen physischen Endpoint besitzt, schlägt das Upgrade auf der virtuellen Master-Appliance fehl. In der Migrationsschnittstelle und im Protokoll wird eine Fehlermeldung angezeigt. Um festzustellen, ob Ihre vRealize Automation 6.2.x-Bereitstellung einen physischen Endpoint besitzt, melden Sie sich bei vRealize Automation als IaaS-Administrator an. Wählen Sie **Infrastruktur > Endpoints** und überprüfen Sie die Liste der Endpoints. Wenn in der Liste ein Platform Type Physical-Endpoint aufgeführt ist, können Sie kein Upgrade auf vRealize Automation 7.0 und höher durchführen.

Physische Endpoints, Reservierungen und virtuelle Maschinenkomponenten in Blueprints werden in vRealize Automation 7.0 und höher nicht unterstützt.

Aktualisierung und Netzwerkprofileinstellungen

Private Netzwerkprofile werden in vRealize Automation 7 und höher nicht unterstützt. Diese Profile werden während des Upgrades ignoriert. Geroutete Netzwerkprofile mit zugeordneten PLR-Edge-Einstellungen werden in vRealize Automation 7 und höher ebenfalls nicht unterstützt. Auch diese Profile werden während des Upgrades ignoriert.

Der private Netzwerkprofiltyp wird in vRealize Automation 7 und höher nicht unterstützt. Wenn während des vRealize Automation-Aktualisierungsvorgangs ein privates Netzwerkprofil in der Quellbereitstellung gefunden wird, wird es ignoriert. Lastausgleichsdienste, die diese privaten Netzwerke referenzieren, werden während der Aktualisierung ebenfalls ignoriert. Die gleichen Aktualisierungsbedingungen gelten für ein geroutetes Netzwerkprofil mit zugeordneten PLR-Edge-Einstellungen. Keine der Netzwerkprofilkonfigurationen wird aktualisiert.

Wenn eine Reservierung ein privates Netzwerkprofil enthält, wird die Einstellung für das private Netzwerkprofil während der Aktualisierung ignoriert. Die Reservierung wird in der Zielbereitstellung als „deaktiviert“ aktualisiert.

Wenn eine Reservierung ein geroutetes Netzwerkprofil mit zugeordneten PLR-Edge-Einstellungen enthält, wird die Spezifikation für geroutete Netzwerkprofile während der Aktualisierung ignoriert. Die Reservierung wird in der Zielbereitstellung als „deaktiviert“ aktualisiert.

Informationen zum Aktualisieren eines Multi-Maschinen-Blueprints mit Netzwerkeinstellungen finden Sie unter [Grundlegendes zum Aktualisieren von Multi-Maschinen-Blueprints](#).

Aktualisierung und berechtigte Aktionen

Sie können kein Upgrade für virtuelle Maschinenaktionen durchführen.

Die Aktionen, die Sie auf bereitgestellten virtuellen Maschinen basierend auf Blueprint-Spezifikationen durchführen können, werden nicht aktualisiert. Um die Aktionen neu zu erstellen, die Sie auf einer virtuellen Maschine durchführen können, passen Sie die Berechtigungen für Blueprints an, sodass nur bestimmte Aktionen zugelassen sind.

Informationen hierzu finden Sie unter [Aktionen in Berechtigungen](#).

Aktualisierung und benutzerdefinierte Eigenschaften

Alle benutzerdefinierten Eigenschaften in vRealize Automation stehen in der aktualisierten Bereitstellung zur Verfügung. Benutzerdefinierte Eigenschaften und Eigenschaftsgruppen werden aktualisiert.

Terminologie und zugehörige Änderungen

Alle Build-Profile, die Sie in der Quellbereitstellung erstellt haben, werden als Eigenschaftsgruppen aktualisiert. Der Begriff *Build-Profil* wird nicht mehr verwendet.

Der Begriff *Eigenschaftensatz* wird nicht mehr verwendet, und die CSV-Eigenschaftensatzdateien sind nicht mehr verfügbar.

Unterscheidung nach Groß-/Kleinschreibung bei benutzerdefinierten Eigenschaftsnamen

Vor vRealize Automation 7.0 war bei den Namen benutzerdefinierter Eigenschaften die Groß-/Kleinschreibung zu beachten. In vRealize Automation 7.0 und höher wird bei benutzerdefinierten Eigenschaftsnamen die Groß-/Kleinschreibung beachtet. Während des Upgrades müssen die Namen benutzerdefinierter Eigenschaften exakt übereinstimmen. Dadurch wird sichergestellt, dass Eigenschaftswerte sich nicht gegenseitig überschreiben und dass sie den Definitionen im Eigenschaftswörterbuch entsprechen. Eine benutzerdefinierte Eigenschaft `hostname` und eine andere benutzerdefinierte Eigenschaft `HOSTNAME` werden in vRealize Automation 7.0 und höher beispielsweise als verschiedene benutzerdefinierte Eigenschaften betrachtet. Die benutzerdefinierte Eigenschaft `hostname` und die benutzerdefinierte Eigenschaft `HOSTNAME` überschreiben sich während des Upgrades nicht gegenseitig.

Leerzeichen in Namen von benutzerdefinierten Eigenschaften

Entfernen Sie vor dem Upgrade auf diese Version von vRealize Automation alle Leerzeichen aus Ihren benutzerdefinierten Eigenschaftsnamen. Ersetzen Sie z. B. das Leerzeichen durch einen Unterstrich, damit die benutzerdefinierte Eigenschaft in der aktualisierten vRealize Automation-Installation erkannt werden kann. Namen benutzerdefinierter Eigenschaften in vRealize Automation dürfen keine Leerzeichen enthalten. Dieses Problem kann sich auch auf die Verwendung einer aktualisierten vRealize Orchestrator-Installation auswirken, die benutzerdefinierte Eigenschaften verwendet, welche in früheren Versionen von vRealize Automation oder vRealize Orchestrator oder beidem Leerzeichen enthielten.

Reservierte Eigenschaftsnamen

Da nun mehrere Schlüsselwörter reserviert sind, können manche aktualisierten Eigenschaften davon betroffen sein. Manche Schlüsselwörter, die vom Blueprint-Code verwendet werden, können importiert werden, z. B. mit den vRealize CloudClient-Blueprint-Importfunktionen. Diese Schlüsselwörter werden als reserviert betrachtet und stehen nicht für Eigenschaften zur Verfügung, die aktualisiert werden. Zu den Schlüsselwörtern zählen u. a. `cpu`, `storage` und `memory`.

Aktualisierung und Application Services

Ein Upgrade der Application Services wird in vRealize Automation 7 oder höher unterstützt.

Nach erfolgreicher Migration auf vRealize Automation 7.4 können Sie das vRealize Automation Application Services-Datenmigrations-Tool für das Upgrade Ihrer Application Services verwenden. Führen Sie diese Schritte aus, um das Tool herunterzuladen.

- 1 Klicken Sie auf [Download VMware vRealize Automation](#).
- 2 Wählen Sie **Treiber & Tools > VMware vRealize Application Services-Migrationstool** aus.

Aktualisierung und Advanced Service Design

Wenn Sie auf vRealize Automation 7 und höher aktualisieren, werden Ihre Advanced Service Design-Elemente zu XaaS-Elementen aktualisiert.

XaaS-Komponenten stehen zur Verwendung auf der Design-Arbeitsfläche zur Verfügung.

Aktualisierung und Blueprint-Preisangaben

Ab Version 7.0 werden vRealize Automation-Preisprofile nicht mehr unterstützt und während der Aktualisierung nicht in die Zielbereitstellung migriert. Sie können die erweiterte Integration mit vRealize Business for Cloud jedoch zum Verwalten Ihrer vRealize Automation-Ressourcenausgaben verwenden.

vRealize Business for Cloud ist jetzt eng in vRealize Automation integriert und unterstützt die folgenden erweiterten Preisgestaltungsfunktionen:

- Einheitlicher Speicherort in vRealize Business for Cloud zum Definieren flexibler Preisgestaltungsrichtlinien für:
 - Infrastrukturressourcen-, Maschinen- und Anwendungs-Blueprints
 - Bereitgestellte virtuelle Maschinen in vRealize Automation für unterstützte Endpoints, wie z. B. vCenter Server, vCloud Director, Amazon Web Services, Azure und OpenStack.
 - Alle operativen Preise, einmaligen Preise und Preise für benutzerdefinierte Eigenschaften von bereitgestellten virtuellen Maschinen
 - Bereitstellungen, die den Preis für virtuelle Maschinen innerhalb der Bereitstellungen enthalten
- Rollenbasierte Kostenauflistungsberichte in vRealize Business for Cloud
- Vollständige Nutzung neuer Funktionen in vRealize Business for Cloud

Vor dem Upgrade können Sie Ihre vorhandenen Ausgabenberichte aus der vRealize Automation-Quellinstanz zu Referenzzwecken exportieren. Nach Abschluss des Upgrades können Sie vRealize Business for Cloud zur Preisgestaltung installieren und konfigurieren.

Hinweis vRealize Automation 7.4 ist nur mit vRealize Business for Cloud 7.4 und höher kompatibel.

Upgrade und Katalogelemente

Nach dem Upgrade von vRealize Automation 6.2.x auf die neueste Version werden manche Katalogelemente im Servicekatalog angezeigt, können jedoch nicht angefordert werden.

Nach der Migration auf die neueste Version von vRealize Automation werden Katalogelemente, die diese Eigenschaftsdefinitionen verwenden, im Servicekatalog angezeigt, können jedoch nicht angefordert werden.

- Steuerungstypen: Kontrollkästchen oder Verknüpfung.
- Attribute: Beziehung, reguläre Ausdrücke oder Eigenschaftslayouts.

In vRealize Automation 7.x werden in Eigenschaftsdefinitionen diese Elemente nicht mehr verwendet. Sie müssen die Eigenschaftsdefinitionen neu erstellen oder sie neu konfigurieren, sodass eine vRealize Orchestrator-Skriptaktion anstelle der eingebetteten Steuerungstypen oder Attribute verwendet wird. Weitere Informationen finden Sie unter [Katalogelemente werden nach dem Upgrade im Servicekatalog aufgeführt, können aber nicht angefordert werden](#).

Checkliste für das Upgrade von vRealize Automation

Wenn Sie ein Upgrade von vRealize Automation 6.2.5 auf 7.4 durchführen, aktualisieren Sie alle vRealize Automation-Komponenten in einer bestimmten Reihenfolge.

Verwenden Sie die Checklisten, um Ihre Arbeit beim Durchführen des Upgrades zu verfolgen. Führen Sie die Aufgaben in der Reihenfolge aus, in der sie vorgegeben werden.

Hinweis Sie müssen die Komponenten in der vorgeschriebenen Reihenfolge aktualisieren und alle Komponenten aktualisieren. Wenn Sie die Reihenfolge nicht einhalten, kann dies zu unerwartetem Verhalten nach dem Upgrade oder zu einem Fehler beim Abschluss des Upgrades führen.

Die Upgrade-Reihenfolge variiert, je nachdem, ob Sie ein Upgrade für eine Minimalumgebung oder eine verteilte Umgebung mit mehreren vRealize Automation-Appliances durchführen.

Tabelle 1-63. Checkliste für das Upgrade einer minimalen vRealize Automation -Umgebung

Aufgabe	Anleitung
<p><input type="checkbox"/> Sichern Sie Ihre aktuelle Installation. Diese Sicherung ist eine wichtige Aufgabe.</p>	<p>Weitere Informationen zum Sichern und Wiederherstellen des Systems finden Sie unter Sichern Ihrer vorhandenen vRealize Automation 6.2.5-Umgebung.</p> <p>Allgemeine Informationen finden Sie im Dokument <i>Configuring Backup and Restore by Using Symantec Netbackup</i> (Konfigurieren der Sicherung und Wiederherstellung unter Verwendung von Symantec Netbackup) unter der Adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-net-backup.pdf.</p>
<p><input type="checkbox"/> Bereiten Sie virtuelle vRealize Automation 6.2.x-Maschinen für das Upgrade vor.</p>	<p>Sie müssen den Knowledgebase-Artikel 51531 durchlesen und alle relevanten Fixes für Ihre Umgebungen vor dem Upgrade durchführen.</p>
<p><input type="checkbox"/> Fahren Sie die Windows-Dienste von vRealize Automation auf Ihrem IaaS-Server herunter.</p>	<p>Siehe Beenden der vRealize Automation-Dienste auf dem IaaS-Windows-Server.</p>
<p><input type="checkbox"/> Wenn der Katalog „Gemeinsame Komponenten“ installiert ist, müssen Sie ihn vor dem Upgrade deinstallieren.</p>	<p>Informationen zum Deinstallieren der Komponenten „Katalog für gemeinsame Komponenten“ finden Sie im <i>Installationshandbuch für den Katalog „Gemeinsame Komponenten“</i>.</p> <p>Falls dieses Handbuch nicht verfügbar ist, führen Sie diese Schritte auf jedem IaaS-Knoten durch.</p> <ol style="list-style-type: none"> 1 Melden Sie sich beim IaaS-Knoten an. 2 Klicken Sie auf Starten. 3 Geben Sie Dienste im Textfeld Programme/Dateien durchsuchen ein. 4 Klicken Sie auf Dienste. 5 Klicken Sie im rechten Fensterbereich des Fensters „Dienste“ mit der rechten Maustaste auf jeden IaaS-Dienst und wählen Sie Beenden aus, um jeden der Dienste zu beenden. 6 Klicken Sie auf Start > Systemsteuerung > Programme und Funktionen. 7 Klicken Sie mit der rechten Maustaste auf jede installierte Komponente im „Katalog für allgemeine Komponenten“ und wählen Sie Deinstallieren. 8 Klicken Sie auf Start > Eingabeaufforderung. 9 Führen Sie in der Eingabeaufforderung iisreset aus.
<p><input type="checkbox"/> Informieren Sie sich über das Upgrade auf diese Version von vRealize Automation, damit Sie wissen, wann ein Upgrade möglich ist und wann nicht, und inwiefern sich aktualisierte Elemente möglicherweise anders verhalten.</p> <p>Nicht für alle Elemente ist ein Upgrade möglich. Darunter fallen Blueprints, Reservierungen und Endpoints. Wenn nicht unterstützte Konfigurationen vorliegen, wird das Upgrade gesperrt.</p>	<p>Siehe Überlegungen zum Upgrade auf diese vRealize Automation-Version.</p>
<p><input type="checkbox"/> Konfigurieren Sie die Hardwareressourcen.</p>	<p>Siehe Erweitern der vCenter Server-Hardwareressourcen für vRealize Automation 6.2.5.</p>

Tabelle 1-63. Checkliste für das Upgrade einer minimalen vRealize Automation -Umgebung (Fortsetzung)

Aufgabe	Anleitung
<input type="checkbox"/> Laden Sie Updates für die vRealize Automation-Appliance herunter.	Siehe Herunterladen von Updates für vRealize Automation-Appliances .
<input type="checkbox"/> Installieren Sie das Update für die vRealize Automation-Appliance.	Siehe Installieren des Updates auf der vRealize Automation-Appliance .
<input type="checkbox"/> Aktualisieren Sie das Single Sign On-Dienstprogramm auf das VMware Identity Manager-Dienstprogramm.	Siehe Ihr Single Sign-On-Kennwort für VMware Identity Manager aktualisieren .
<input type="checkbox"/> Aktualisieren Sie den Lizenzschlüssel.	Siehe Aktualisieren des Lizenzschlüssels .
<input type="checkbox"/> Migrieren Sie die Identitätsquelle auf den VMware Identity Manager.	Migrieren von Identitätsquellen auf VMware Identity Manager
<input type="checkbox"/> Führen Sie ein Upgrade der IaaS-Komponenten durch.	Siehe Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation .
<input type="checkbox"/> Aktualisieren Sie die externe vRealize Orchestrator-Instanz.	Siehe Upgrade einer eigenständigen vRealize Orchestrator Appliance für die Verwendung mit vRealize Automation . Siehe Upgrade eines externen vRealize Orchestrator Appliance-Clusters für die Verwendung mit vRealize Automation .
<input type="checkbox"/> Fügen Sie Benutzer oder Gruppen zu einer Active Directory-Verbindung hinzu.	Siehe Hinzufügen von Benutzern oder Gruppen zu einer Active Directory-Verbindung .

Tabelle 1-64. Checkliste für das Upgrade einer verteilten vRealize Automation -Umgebung

Aufgabe	Anleitung
<input type="checkbox"/> Sichern Sie Ihre aktuelle Installation. Diese Sicherung ist eine wichtige Aufgabe.	Weitere Informationen zum Sichern und Wiederherstellen des Systems finden Sie unter Sichern Ihrer vorhandenen vRealize Automation 6.2.5-Umgebung . Detaillierte Informationen finden Sie im Dokument <i>Configuring Backup and Restore by Using Symantec Netbackup</i> (Konfigurieren der Sicherung und Wiederherstellung unter Verwendung von Symantec Netbackup) unter der Adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-net-backup.pdf .
<input type="checkbox"/> Bereiten Sie virtuelle vRealize Automation 6.2.x-Maschinen für das Upgrade vor.	Sie müssen den Knowledgebase-Artikel 51531 durchlesen und alle relevanten Fixes für Ihre Umgebungen vor dem Upgrade durchführen.
<input type="checkbox"/> Fahren Sie die vRealize Automation-Dienste auf Ihren IaaS-Windows-Servern herunter.	Siehe Beenden der vRealize Automation-Dienste auf dem IaaS-Windows-Server .

Tabelle 1-64. Checkliste für das Upgrade einer verteilten vRealize Automation -Umgebung (Fortsetzung)

Aufgabe	Anleitung
<p><input type="checkbox"/> Wenn der Katalog „Gemeinsame Komponenten“ installiert ist, müssen Sie ihn vor dem Upgrade deinstallieren.</p>	<p>Informationen zum Deinstallieren der Komponenten „Katalog für gemeinsame Komponenten“ finden Sie im <i>Installationshandbuch für den Katalog „Gemeinsame Komponenten“</i>.</p> <p>Falls dieses Handbuch nicht verfügbar ist, führen Sie diese Schritte auf jedem IaaS-Knoten durch.</p> <ol style="list-style-type: none"> 1 Melden Sie sich beim IaaS-Knoten an. 2 Klicken Sie auf Starten. 3 Geben Sie Dienste im Textfeld Programme/Dateien durchsuchen ein. 4 Klicken Sie auf Dienste. 5 Klicken Sie im rechten Fensterbereich des Fensters „Dienste“ mit der rechten Maustaste auf jeden IaaS-Dienst und wählen Sie Beenden aus, um jeden der Dienste zu beenden. 6 Klicken Sie auf Start > Systemsteuerung > Programme und Funktionen. 7 Klicken Sie mit der rechten Maustaste auf jede installierte Komponente im „Katalog für allgemeine Komponenten“ und wählen Sie Deinstallieren. 8 Klicken Sie auf Start > Eingabeaufforderung. 9 Führen Sie in der Eingabeaufforderung <code>iisreset</code> aus.
<p><input type="checkbox"/> Konfigurieren Sie die Hardwareressourcen für das Upgrade.</p>	<p>Siehe Erweitern der vCenter Server-Hardwareressourcen für vRealize Automation 6.2.5.</p>
<p><input type="checkbox"/> Deaktivieren Sie Ihre Lastausgleichsmodule.</p>	<p>Deaktivieren Sie jeden sekundären Knoten und entfernen Sie die Überwachung des Systemzustands von vRealize Automation für die folgenden Elemente:</p> <ul style="list-style-type: none"> ■ vRealize Automation-Appliance ■ IaaS-Website ■ IaaS Manager Service <p>Stellen Sie für ein erfolgreiches Upgrade Folgendes sicher:</p> <ul style="list-style-type: none"> ■ Der Datenverkehr des Lastausgleichsdienstes wird nur an den primären Knoten weitergeleitet. ■ Die vRealize Automation-Systemüberwachung für die Appliance, die Website und den Manager Service wurde entfernt.
<p><input type="checkbox"/> Laden Sie Updates für die vRealize Automation-Appliance herunter.</p>	<p>Siehe Herunterladen von Updates für vRealize Automation-Appliances.</p>
<p><input type="checkbox"/> Installieren Sie das Update auf der ersten vRealize Automation-Appliance in Ihrer Installation. Wenn Sie eine Appliance als Master festgelegt haben, aktualisieren Sie diese Appliance zuerst.</p>	<p>Siehe Installieren des Updates auf der vRealize Automation-Appliance.</p>
<p><input type="checkbox"/> Aktualisieren Sie das Single Sign On-Dienstprogramm auf das VMware Identity Manager-Dienstprogramm.</p>	<p>Siehe Ihr Single Sign-On-Kennwort für VMware Identity Manager aktualisieren.</p>

Tabelle 1-64. Checkliste für das Upgrade einer verteilten vRealize Automation -Umgebung (Fortsetzung)

Aufgabe	Anleitung
<input type="checkbox"/> Aktualisieren Sie den Lizenzschlüssel.	Siehe Aktualisieren des Lizenzschlüssels .
<input type="checkbox"/> Migrieren Sie die Identitätsquelle auf das VMware Identity Manager-Dienstprogramm.	Migrieren von Identitätsquellen auf VMware Identity Manager
<input type="checkbox"/> Installieren Sie das Update auf den restlichen vRealize Automation-Appliances.	Installieren des Updates auf zusätzlichen vRealize Automation-Appliances
<input type="checkbox"/> Führen Sie ein Upgrade der IaaS-Komponenten durch.	Siehe Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation .
<input type="checkbox"/> Aktualisieren Sie die externe vRealize Orchestrator-Instanz.	Siehe Upgrade einer eigenständigen vRealize Orchestrator Appliance für die Verwendung mit vRealize Automation . Siehe Upgrade eines externen vRealize Orchestrator Appliance-Clusters für die Verwendung mit vRealize Automation .
<input type="checkbox"/> Aktivieren Sie die Lastausgleichsdienste.	Aktivieren der Lastausgleichsdienste

Benutzeroberflächen der vRealize Automation -Umgebung

Sie verwenden und verwalten Ihre vRealize Automation-Umgebung mit mehreren Schnittstellen.

Benutzeroberfläche

In diesen Tabellen werden die Schnittstellen beschrieben, die Sie zum Verwalten Ihrer vRealize Automation-Umgebung verwenden

Tabelle 1-65. vRealize Automation Verwaltungskonsole

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die vRealize Automation-Konsole für diese Systemadministrationsaufgaben.</p> <ul style="list-style-type: none"> ■ Mandanten hinzufügen. ■ vRealize Automation-Benutzeroberfläche anpassen. ■ E-Mail-Server konfigurieren. ■ Ereignisprotokolle anzeigen. ■ Konfigurieren Sie vRealize Orchestrator. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf vRealize Automation-Konsole. Sie können auch diese URL zum Öffnen der vRealize Automation-Konsole verwenden: <code>https://vra-va-hostname.domain.name/vcac</code> 3 Melden Sie sich an. 	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle sein.</p>

Tabelle 1-66. vRealize Automation -Mandantenkonsole. Diese Schnittstelle ist die primäre Benutzeroberfläche, mit der Sie Ihre Dienste und Ressourcen erstellen und verwalten.

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden vRealize Automation für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Neue IT-Dienst-Blueprints anfordern. ■ Cloud- und IT-Ressourcen erstellen und verwalten. ■ Benutzerdefinierte Gruppen erstellen und verwalten. ■ Erstellt und verwaltet Business-Gruppen. ■ Rollen zu Benutzern zuweisen. 	<p>1 Starten Sie einen Browser und geben Sie die URL für Ihren Mandanten mit dem vollqualifizierten Domännennamen der virtuelle Appliance und dem Namen der Mandanten-URL ein.</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name .</code></p> <p>2 Melden Sie sich an.</p>	<p>Sie müssen ein Benutzer mit mindestens einer dieser Rollen sein:</p> <ul style="list-style-type: none"> ■ Anwendungsarchitekt ■ Genehmigungsadministrator ■ Katalog-Administrator ■ Container-Administrator ■ Container-Architekt ■ Health Consumer ■ Infrastrukturarchitekt ■ Sicherer Export, Verbraucher ■ Softwarearchitekt ■ Mandantenadministrator ■ XaaS-Architekt

Tabelle 1-67. Verwaltung der vRealize Automation -Appliance Diese Schnittstelle wird manchmal als „Virtual Appliance Management Interface“ (VAMI) bezeichnet.

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Verwaltung der vRealize Automation-Appliance für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Status der registrierte Dienste anzeigen. ■ Systeminformationen anzeigen und die Appliance neu starten oder herunterfahren. ■ Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit verwalten. ■ Netzwerkstatus anzeigen. ■ Updatestatus anzeigen und Updates installieren. ■ Administrationseinstellungen verwalten. ■ vRealize Automation-Hosteinstellungen verwalten. ■ SSO-Einstellungen verwalten. ■ Lizenzen verwalten. ■ vRealize Automation-Postgres-Datenbank konfigurieren. ■ vRealize Automation-Meldungen konfigurieren. ■ vRealize Automation-Protokollierung konfigurieren. ■ IaaS-Komponenten installieren. ■ Von einer vorhandenen vRealize Automation-Installation migrieren. ■ IaaS-Komponentenzertifikate verwalten. ■ Xenon-Dienst konfigurieren. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance. Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code> 3 Melden Sie sich an. 	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance eingegebene Kennwort.

Tabelle 1-68. vRealize Orchestrator -Client

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden den vRealize Orchestrator-Client für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Aktionen entwickeln. ■ Workflows entwickeln. ■ Richtlinien verwalten. ■ Pakete installieren. ■ Berechtigungen für Benutzer und Benutzergruppen verwalten. ■ Tags an URI-Objekte anhängen. ■ Bestandsliste anzeigen. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die vRealize Automation-Begrüßungsseite mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Um die Datei „client.jnlp“ auf Ihren lokalen Computer zu laden, klicken Sie auf vRealize Orchestrator-Client. 3 Klicken Sie mit der rechten Maustaste auf die <code>client.jnlp</code>-Datei und wählen Sie Starten aus. 4 Klicken Sie im Dialogfeld „Möchten Sie fortfahren“ auf Weiter. 5 Melden Sie sich an. 	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle oder Mitglied der Gruppe „vcoadmins“ in den Authentifizierungsanbieter-Einstellungen im vRealize Orchestrator-Control Center sein.</p>

Tabelle 1-69. vRealize Orchestrator Control Center

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden das vRealize Orchestrator Control Center, um die Konfiguration der vRealize Orchestrator-Standardinstanz zu bearbeiten, die in vRealize Automation eingebettet ist.</p>	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance. Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code> 3 Melden Sie sich an. 4 Klicken Sie auf vRA-Einstellungen > Orchestrator. 5 Wählen Sie Orchestrator-Benutzeroberfläche aus. 6 Klicken Sie auf Starten. 7 Klicken Sie auf die URL für die Orchestrator-Benutzeroberfläche. 8 Melden Sie sich an. 	<p>Benutzername</p> <ul style="list-style-type: none"> ■ Geben Sie root ein, wenn keine rollenbasierte Authentifizierung konfiguriert ist. ■ Geben Sie Ihren vRealize Automation-Benutzernamen ein, wenn dieser für die rollenbasierte Authentifizierung konfiguriert ist. <p>Kennwort</p> <ul style="list-style-type: none"> ■ Geben Sie das Kennwort ein, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben, wenn die rollenbasierte Authentifizierung nicht konfiguriert ist. ■ Geben Sie das Kennwort für Ihren Benutzernamen ein, wenn Ihr Benutzername für die rollenbasierte Authentifizierung konfiguriert ist.

Tabelle 1-70. Linux-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Linux-Befehlszeile auf einem Host, z. B. auf dem Host der vRealize Automation-Appliance Host, für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Dienste starten oder beenden ■ Konfigurationsdateien bearbeiten ■ Befehle ausführen ■ Daten abrufen 	<p>1 Öffnen Sie auf dem Host der vRealize Automation-Appliance eine neue Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile auf Ihrem lokalen Computer zu öffnen, ist das Starten einer Sitzung auf dem Host mit einer Anwendung, zum Beispiel PuTTY.</p> <p>2 Melden Sie sich an.</p>	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance erstellt Kennwort.

Tabelle 1-71. Windows-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Wie können eine Windows-Eingabeaufforderung auf einem Host verwenden z. B. auf dem IaaS-Host, um Skripts ausführen.</p>	<p>1 Melden Sie sich auf dem IaaS-Host bei Windows an.</p> <p>Eine Möglichkeit, sich über Ihren lokalen Computer anzumelden, ist das Starten einer Remote-Desktop-Sitzung.</p> <p>2 Öffnen Sie die Windows-Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile zu öffnen, ist das Klicken mit der rechten Maustaste auf das Startsymbol auf dem Host und die Auswahl von Eingabeaufforderung oder Eingabeaufforderung (Admin).</p>	<ul style="list-style-type: none"> ■ Benutzername: Benutzer mit Administratorrechten. ■ Kennwort: Kennwort des Benutzers.

Upgrade von in vRealize Automation integrierten VMware -Produkten

Beim Upgrade von vRealize Automation müssen Sie alle in Ihre vRealize Automation-Umgebung integrierten VMware-Produkte verwalten.

Wenn Ihre vRealize Automation-Umgebung in ein oder mehrere zusätzliche Produkte integriert ist, sollten Sie ein Upgrade von vRealize Automation vornehmen, bevor Sie zusätzliche Produkte aktualisieren.

Wenn vRealize Business for Cloud in vRealize Automation integriert ist, müssen Sie die Registrierung von vRealize Business for Cloud vor dem Upgrade von vRealize Automation aufheben.

Folgen Sie dem vorgeschlagenen Workflow für die Verwaltung von integrierten Produkten beim Upgrade von vRealize Automation.

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von VMware vRealize Operations Manager durch.
- 3 Führen Sie ein Upgrade von VMware vRealize Log Insight durch.
- 4 Führen Sie ein Upgrade von VMware vRealize Business for Cloud durch.

Dieser Abschnitt bietet zusätzliche Unterstützung für die Verwaltung von vRealize Business for Cloud bei Integration in Ihre vRealize Automation-Umgebung.

Upgrade von einer in vRealize Automation integrierten vRealize Operations Manager - Instanz

Führen Sie nach dem Upgrade von vRealize Automation ein Upgrade von vRealize Operations Manager aus.

Verfahren

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von vRealize Operations Manager durch. Informationen finden Sie unter *Aktualisieren Ihrer Software* in der [VMware vRealize Operations Manager-Dokumentation](#).

Upgrade von einer in vRealize Automation integrierten vRealize Log Insight -Instanz

Führen Sie nach dem Upgrade von vRealize Automation ein Upgrade von vRealize Log Insight aus.

Verfahren

- 1 Führen Sie ein Upgrade von vRealize Automation durch.
- 2 Führen Sie ein Upgrade von vRealize Log Insight durch. Informationen hierzu finden Sie unter *Aktualisieren von vRealize Log Insight* in der [VMware vRealize Log Insight-Dokumentation](#).

Upgrade von einer in vRealize Automation integrierten vRealize Business for Cloud -Instanz

Wenn Sie Ihre vRealize Automation-Umgebung aktualisieren, müssen Sie die Registrierung Ihrer Verbindung zu vRealize Business for Cloud aufheben und erneut registrieren.

Führen Sie diesen Vorgang aus, um die Kontinuität des vRealize Business for Cloud-Diensts beim Upgrade Ihrer vRealize Automation-Umgebung sicherzustellen.

Verfahren

- 1 Aufheben der Registrierung von vRealize Business for Cloud für vRealize Automation. Weitere Informationen finden Sie unter *Aufheben der Registrierung von vRealize Business for Cloud für vRealize Automation* in der [VMware vRealize Business for Cloud-Dokumentation](#).
- 2 Führen Sie ein Upgrade von vRealize Automation durch.
- 3 Falls erforderlich, aktualisieren Sie vRealize Business for Cloud. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Business for Cloud* in der [VMware vRealize Business for Cloud-Dokumentation](#).
- 4 Registrieren Sie vRealize Business for Cloud bei vRealize Automation. Weitere Informationen finden Sie unter *Registrieren von vRealize Business for Cloud bei vRealize Automation* in der [VMware vRealize Business for Cloud-Dokumentation](#).

Vorbereiten des vRealize Automation -Upgrades

Sie müssen verschiedene Aufgaben und Verfahren durchführen, bevor Sie ein Upgrade von vRealize Automation von Version 6.2.5 auf Version 7.4 durchführen können.

Führen Sie die Aufgaben in der Reihenfolge aus, in der sie in der Checkliste angezeigt werden. Siehe [Checkliste für das Upgrade von vRealize Automation](#).

Voraussetzungen für ein Backup für das Upgrade von vRealize Automation

Schließen Sie die Voraussetzungen für das Backup ab, bevor Sie ein Upgrade von vRealize Automation 6.2.5 auf 7.4. durchführen.

Voraussetzungen

- Überprüfen Sie, ob die Quellumgebung vollständig installiert und konfiguriert wurde.
- Sichern Sie für jede Appliance in der Quellumgebung alle Konfigurationsdateien der vRealize Automation-Appliance in folgenden Verzeichnissen:
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Sichern Sie die externen Workflow-Konfigurationsdateien (Xmldb) von vRealize Automation auf dem System. Speichern Sie die Sicherungsdateien in einem temporären Verzeichnis. Diese Dateien befinden sich unter `VMware\VCa\Server\ExternalWorkflows\xmldb\`. Sie können die xmldb-Dateien auf dem neuen System nach der Migration wiederherstellen. Siehe [Wiederherstellen von Dateien für die Zeitüberschreitung bei externen Workflows](#).

Informationen zu einem in diesem Zusammenhang auftretenden Problem finden Sie unter [Sicherungskopien von XML-Dateien führen zu einer Zeitüberschreitung des Systems](#).

- Sichern Sie die externe PostgreSQL-Datenbank von vRealize Automation. Um festzustellen, ob eine externe PostgreSQL-Datenbank vorliegt, führen Sie diese Schritte durch.
 - a Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen `https://va-hostname.domain.name:5480` an.

In einer verteilten Umgebung melden Sie sich bei der primären Verwaltungskonsole der vRealize Automation-Appliance an.
 - b Wählen Sie **vRA-Einstellungen > Datenbank** aus.
 - c Wenn sich der vRealize Automation-PostgreSQL-Datenbank-Knoten-Host vom Host der vRealize Automation-Appliance unterscheidet, sichern Sie die Datenbank. Wenn der Datenbank-Knoten-Host mit dem Host der Appliance identisch ist, müssen Sie die Datenbank nicht sichern.

Informationen zum Sichern der PostgreSQL-Datenbank finden Sie unter <https://www.postgresql.org/>.
- Erstellen Sie einen Snapshot Ihrer Mandantenkonfiguration und der zugewiesenen Benutzer.
- Sichern Sie alle von Ihnen angepassten Dateien, wie zum Beispiel `DataCenterLocations.xml`.
- Erstellen Sie einen Snapshot aller virtuellen Appliances und IaaS-Server. Halten Sie die üblichen Richtlinien für das Sichern des gesamten Systems ein, falls das Upgrade von vRealize Automation fehlschlägt. Siehe [Sicherung und Wiederherstellung für vRealize Automation-Installationen](#).

Sichern Ihrer vorhandenen vRealize Automation 6.2.5-Umgebung

Fahren Sie vor dem Upgrade Ihre vRealize Automation 6.2.5-Umgebungskomponenten herunter und erstellen Sie einen Snapshot.

Erstellen Sie vor dem Upgrade einen Snapshot dieser Komponenten, während das System ausgeschaltet ist.

- vRealize Automation-IaaS-Server (Windows-Knoten)
- vRealize Automation-Appliances (Linux-Knoten)
- vRealize Automation-(SSO)-Identitätsknoten

Wenn das Upgrade fehlschlägt, kehren Sie über den Snapshot zur letzten bekannten fehlerfreien Konfiguration zurück und versuchen Sie ein erneutes Upgrade.

Voraussetzungen

- Überprüfen Sie, ob sich die eingebettete PostgreSQL-Datenbank im Hochverfügbarkeitsmodus befindet. Suchen Sie in diesem Fall den aktuellen Master-Knoten. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel <http://kb.vmware.com/kb/2105809>.
- Wenn Ihre Umgebung über eine PostgreSQL Datenbank verfügt, erstellen Sie eine Datenbank-Sicherungsdatei.
- Wenn die vRealize Automation Microsoft SQL-Datenbank nicht auf dem IaaS-Server gehostet wird, erstellen Sie eine Datenbanksicherungsdatei. Suchen Sie im [Microsoft Developer Network](#) nach Artikeln zur Erstellung einer vollständigen SQL Server-Datenbanksicherung, um weitere Informationen zu erhalten.
- Überprüfen Sie, ob die Sicherungsvoraussetzungen für das Upgrade erfüllt sind.
- Überprüfen Sie, ob ein Snapshot des Systems erstellt wurde, während es heruntergefahren war. Die ist die empfohlene Methode, einen Snapshot zu erstellen. Informationen hierzu finden Sie in der *vSphere 6.0-Dokumentation*.

Hinweis Wenn Sie die vRealize Automation-Appliance und die IaaS-Komponenten sichern, deaktivieren Sie speicherinterne und stillgelegte Snapshots.

- Wenn Sie die Datei `app.config` geändert haben, erstellen Sie eine Sicherung dieser Datei. Siehe [Wiederherstellung von vorgenommenen Änderungen an der Protokollierung in der app.config-Datei](#).
- Erstellen Sie eine Sicherung der externen Workflow-Konfigurationsdateien (xmldb). Siehe [Wiederherstellen von Dateien für die Zeitüberschreitung bei externen Workflows](#).
- Stellen Sie sicher, dass Sie über einen Speicherort außerhalb des aktuellen Ordners verfügen, an dem Sie die Sicherungsdatei speichern können. Siehe [Sicherungskopien von XML-Dateien führen zu einer Zeitüberschreitung des Systems](#).

Verfahren

- 1 Melden Sie sich bei Ihrem vCenter Server an.

- 2 Suchen Sie nach diesen 6.2.5-Komponenten.vRealize Automation
 - vRealize Automation-aaS-Server (Windows-Knoten)
 - vRealize Automation-Appliances (Linux-Knoten)
 - vRealize Automation-(SSO)-Identitätsknoten
- 3 Fahren Sie die unten aufgeführten virtuellen Maschinen herunter, indem Sie jede einzeln auswählen, auf **Gast herunterfahren** klicken und warten, bis die virtuelle Maschine stoppt. Gehen Sie dabei in der folgenden Reihenfolge vor:
 - a virtuelleaaS-Proxy-Agent-Maschinen
 - b virtuelle DEM Worker-Maschinen
 - c virtuelle DEM Orchestrator-Maschine
 - d virtuelle Manager Service-Maschine
 - e virtuelle Webservice-Maschinen
 - f Sekundäre virtuelle vRealize Automation-Appliances
 - g Primäre virtuelle vRealize Automation-Appliance
 - h virtuelle Manager-Maschinen (sofern vorhanden)
 - i Identity Appliance
- 4 Erstellen Sie einen Snapshot von jeder vRealize Automation 6.2.5-VM.
- 5 Klonen Sie jeden vRealize Automation-Appliance-Knoten.

Führen Sie das Upgrade auf den geklonten virtuellen Maschinen durch.
- 6 Schalten Sie jede ursprüngliche virtuelle vRealize Automation-Appliance-Maschine aus, bevor Sie einen Upgrade der geklonten virtuellen Maschinen durchführen.

Lassen Sie die ursprünglichen VMs ausgeschaltet und verwenden Sie sie nur dann, wenn Sie das System wiederherstellen müssen.

Nächste Schritte

[Erweitern der vCenter Server-Hardwareressourcen für vRealize Automation 6.2.5.](#)

Erweitern der vCenter Server -Hardwareressourcen für vRealize Automation 6.2.5

Bevor Sie das Upgrade von vRealize Automation 6.2.5 durchführen, müssen Sie die Hardwareressourcen für jede vRealize Automation-Appliance erweitern.

Bei diesem Verfahren wird davon ausgegangen, dass Sie den Windows-vCenter Server-Client verwenden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Klon jeder vRealize Automation-Appliance verfügen.

- Stellen Sie sicher, dass Sie für jeden Appliance-Klon über mindestens 140 GB freien Speicherplatz in Ihrem vCenter Server verfügen.
- Stellen Sie sicher, dass die ursprünglichen Appliances ausgeschaltet sind.

Verfahren

- 1 Melden Sie sich bei vCenter Server an.
- 2 Klicken Sie mit der rechten Maustaste auf das Symbol einer geklonten vRealize Automation-Appliance und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Arbeitsspeicher** aus und legen Sie den Wert auf 18 GB fest.
- 4 Wählen Sie **CPU** aus und legen Sie die **Anzahl der virtuellen Sockets** auf 4 fest.
- 5 Erweitern Sie die Größe der virtuellen Festplatte 1 auf 50 GB.
 - a Wählen Sie Festplatte 1 aus.
 - b Ändern Sie die Größe in 50 GB.
 - c Klicken Sie auf **OK**.
- 6 Wenn keine Festplatte 3 vorhanden ist, führen Sie diese Schritte durch, um eine Festplatte 3 mit einer Größe von 25 GB hinzuzufügen.
 - a Klicken Sie auf **Hinzufügen** über der Ressourcentabelle, um eine virtuelle Festplatte hinzuzufügen.
 - b Wählen Sie **Festplatte** für den **Gerätetyp** aus und klicken Sie auf **Weiter**.
 - c Wählen Sie **Neue virtuelle Festplatte erstellen** aus und klicken Sie auf **Weiter**.
 - d Legen Sie als Festplattengröße **25 GB** fest.
 - e Wählen Sie **Gemeinsam mit virtueller Maschine speichern** aus und klicken Sie auf **Weiter**.
 - f Stellen Sie sicher, dass die Option **Unabhängig** für **Modus** deaktiviert und **SCSI (0:2)** für **Virtueller Gerätemodus** ausgewählt ist, und klicken Sie auf **Weiter**.

Wenn Sie aufgefordert werden, die empfohlenen Einstellungen zu übernehmen, akzeptieren Sie diese.
 - g Klicken Sie auf **Fertig stellen**.
 - h Klicken Sie auf **OK**.
- 7 Falls eine virtuelle Festplatte 4 aus einer früheren vRealize Automation-Version vorhanden ist, führen Sie diese Schritte durch.
 - a Schalten Sie den Klon der primären virtuellen Appliance ein und warten Sie etwa eine Minute.
 - b Schalten Sie den Klon der sekundären virtuellen Appliance ein.
 - c Öffnen Sie auf dem Klon der primären virtuellen Appliance eine neue Eingabeaufforderung und wechseln Sie zu `/etc/fstab`.

- d Öffnen Sie auf dem Klon der primären virtuellen Appliance die `fstab`-Datei und entfernen Sie die mit `/dev/sdd` beginnenden Zeilen, die die Write-Ahead-Protokolle (`Wal_Archive`) enthalten.
 - e Speichern Sie die Datei auf dem Klon der primären virtuellen Appliance.
 - f Öffnen Sie auf dem Klon der sekundären virtuellen Appliance eine neue Eingabeaufforderung und wechseln Sie zu `/etc/fstab`.
 - g Öffnen Sie auf dem Klon der sekundären virtuellen Appliance die `fstab`-Datei und entfernen Sie die mit `/dev/sdd` beginnenden Zeilen, die die Write-Ahead-Protokolle (`Wal_Archive`) enthalten.
 - h Speichern Sie die Datei auf dem Klon der sekundären virtuellen Appliance.
 - i Schalten Sie den Klon der sekundären virtuellen Appliance aus und warten Sie etwa eine Minute.
 - j Schalten Sie den Klon der primären virtuellen Appliance aus.
 - k Klicken Sie mit der rechten Maustaste auf das Symbol der geklonten primären vRealize Automation-Appliance und wählen Sie **Einstellungen bearbeiten** aus.
 - l Löschen Sie die Festplatte 4 von der geklonten primären virtuellen Appliance-Maschine.
 - m Klicken Sie mit der rechten Maustaste auf das Symbol der geklonten sekundären vRealize Automation-Appliance und wählen Sie **Einstellungen bearbeiten** aus.
 - n Löschen Sie die Festplatte 4 von der geklonten sekundären virtuellen Appliance-Maschine.
- 8 Führen Sie diese Schritte durch, um eine Festplatte 4 mit einer Größe von 50 GB zur geklonten primären und sekundären virtuellen Appliance-Maschine hinzuzufügen.
- a Klicken Sie auf **Hinzufügen** über der Ressourcentabelle, um eine virtuelle Festplatte hinzuzufügen.
 - b Wählen Sie **Festplatte** für den **Gerätetyp** aus und klicken Sie auf **Weiter**.
 - c Wählen Sie **Neue virtuelle Festplatte erstellen** aus und klicken Sie auf **Weiter**.
 - d Legen Sie als Festplattengröße **50 GB** fest.
 - e Wählen Sie **Gemeinsam mit virtueller Maschine speichern** aus und klicken Sie auf **Weiter**.
 - f Stellen Sie sicher, dass die Option **Unabhängig** für **Modus** deaktiviert und **SCSI (0:3)** für **Virtualer Gerätemodus** ausgewählt ist. Klicken Sie anschließend auf **Weiter**.
Wenn Sie aufgefordert werden, die empfohlenen Einstellungen zu übernehmen, akzeptieren Sie diese.
 - g Klicken Sie auf **Fertig stellen**.
 - h Klicken Sie auf **OK**.
- 9 Erstellen Sie einen Snapshot der geklonten primären virtuellen Appliance-Maschine und der geklonten sekundären virtuellen Appliance-Maschine.

Nächste Schritte

[Einschalten des gesamten Systems.](#)

Einschalten des gesamten Systems

Nachdem Sie die vCenter-Hardwareressourcen für ein Upgrade erhöht haben, schalten Sie vor dem Ausführen des Upgrades das System ein.

Voraussetzungen

- [Sichern Ihrer vorhandenen vRealize Automation 6.2.5-Umgebung.](#)
- [Erweitern der vCenter Server-Hardwareressourcen für vRealize Automation 6.2.5.](#)

Verfahren

- 1 Schalten Sie das gesamte System ein.

Anweisungen finden Sie in der vRealize Automation 6.2-Version des Themas [Starten von vRealize Automation.](#)

Hinweis Verwenden Sie in einer Hochverfügbarkeitsumgebung dieses Verfahren zum Einschalten der virtuellen Appliances.

- a Schalten Sie die virtuelle Appliance ein, die Sie zuletzt ausgeschaltet haben.
- b Warten Sie eine Minute.
- c Schalten Sie die verbleibenden virtuellen Appliances ein.

-
- 2 Überprüfen Sie, ob das System voll funktionsfähig ist.

Nächste Schritte

[Beenden der vRealize Automation-Dienste auf dem IaaS-Windows-Server.](#)

Beenden der vRealize Automation -Dienste auf dem IaaS -Windows-Server

Bei Bedarf können Sie das folgende Verfahren verwenden, um vRealize Automation-Dienste auf jedem Server zu beenden, der IaaS-Dienste ausführt.

Beenden Sie vor Beginn des Upgrades die vRealize Automation-Dienste auf jedem IaaS Windows-Server.

Hinweis Außer für eine passive Sicherungsinstanz des Manager Service muss der Starttyp für alle Dienste während des Upgrades auf „Automatisch“ eingestellt sein. Wenn Sie den Starttyp für die Dienste auf „Manuell“ festlegen, schlägt der Upgrade-Vorgang fehl.

Verfahren

- 1 Melden Sie sich bei Ihrem IaaS-Windows-Server an.
- 2 Wählen Sie **Start > Verwaltung > Dienste** aus.

- 3 Beenden Sie die Dienste in der folgenden Reihenfolge. Achten Sie darauf, die virtuelle Maschine selbst nicht herunterzufahren.

Jede virtuelle Maschine verfügt über einen Management-Agent, der mit jedem Satz von Diensten gestoppt werden muss.

- a Jeder VMware vCloud Automation Center-Agent
- b Jeder VMware DEM-Worker
- c Der VMware DEM-Orchestrator
- d Der VMware vCloud Automation Center-Dienst

- 4 Deaktivieren Sie bei verteilten Bereitstellungen mit Lastausgleichsdiensten alle sekundären Knoten und entfernen Sie die Überwachung des Systemzustands von vRealize Automation für die folgenden Elemente.

- a vRealize Automation-Appliance
- b IaaS-Website
- c IaaS-Manager-Dienst

Stellen Sie sicher, dass der Datenverkehr des Lastausgleichsdienstes nur zu den primären Knoten geleitet wird und dass die vRealize Automation-Systemüberwachung für die Appliance, die Website und den Manager-Dienst entfernt wird, damit das Upgrade nicht fehlschlägt.

- 5 Überprüfen Sie mithilfe der folgenden Schritte, ob der in Microsoft Internetinformationsdienste (Internet Information Services, IIS) gehostete IaaS-Dienst ausgeführt wird.

- a Navigieren Sie in Ihrem Browser zur URL **https://webhostname/Repository/Data/MetaModel.svc**, um zu überprüfen, ob das Web-Repository ausgeführt wird. Wenn die Überprüfung erfolgreich ist, werden keine Fehler zurückgegeben und eine Liste der Modelle wird im XML-Format angezeigt.
- b Überprüfen Sie den in der Datei „Repository.log“ im Webknoten der virtuellen IaaS-Maschine aufgezeichneten Status und ermitteln Sie, ob der Status „OK“ zurückgemeldet wird. Die Datei ist im VCAC-Basisordner unter `/Server/Model Manager Web/Logs/Repository.log` gespeichert.

Melden Sie sich im Fall einer verteilten IaaS-Website bei der sekundären Website an (ohne MMD) und halten Sie den Microsoft IIS-Server vorübergehend an. Überprüfen Sie die Konnektivität von „MetaModel.svc“. Um sicherzustellen, dass der Datenverkehr des Lastausgleichs nur über den primären Webknoten geleitet wird, starten Sie den Microsoft IIS-Server.

Nächste Schritte

[Herunterladen von Updates für vRealize Automation-Appliances.](#)

Herunterladen von Updates für vRealize Automation -Appliances

In der Verwaltungskonsole Ihrer Appliance können Sie nach Updates suchen und die Updates mit einer der folgenden Methoden herunterladen.

Die beste Leistung lässt sich bei Upgrades mit der ISO-Dateimethode erzielen.

Um mögliche Probleme bei der Aktualisierung Ihrer Appliance oder bei Problemen während der Aktualisierung der Appliance zu vermeiden, lesen Sie den [VMware-Knowledgebase-Artikel vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database \(54987\)](#) (vRealize Automation-Upgrade schlägt aufgrund von Duplikaten in der vRealize Orchestrator-Datenbank fehl).

- [Herunterladen von Updates für vRealize Automation-Appliances aus einem VMware-Repository](#)

Sie können das Update für Ihre vRealize Automation-Appliance aus einem öffentlichen Repository auf der vmware.com-Website herunterladen.

- [Herunterladen von Updates für virtuelle Appliances zur Verwendung mit einem CD-ROM-Laufwerk](#)

Sie können Ihre virtuelle Appliance von einer ISO-Datei aktualisieren, die die Appliance vom virtuellen CD-ROM-Laufwerk liest. Dies ist die bevorzugte Methode.

Herunterladen von Updates für vRealize Automation -Appliances aus einem VMware -Repository

Sie können das Update für Ihre vRealize Automation-Appliance aus einem öffentlichen Repository auf der vmware.com-Website herunterladen.

Voraussetzungen

- Sichern Sie Ihre vorhandene vRealize Automation-Umgebung.
- Stellen Sie sicher, dass die vRealize Automation-Appliance eingeschaltet ist.

Verfahren

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 2 Klicken Sie auf die Registerkarte **Update**.
- 3 Klicken Sie auf **Einstellungen**.
- 4 (Optional) Legen Sie im Bereich „Automatische Updates“ fest, wie oft nach Updates gesucht werden soll.
- 5 Wählen Sie im Bereich „Update-Repository“ die Option **Standard-Repository verwenden** aus.
Das Standard-Repository wird auf die korrekte VMware.com-URL festgelegt.
- 6 Klicken Sie auf **Einstellungen speichern**.

Herunterladen von Updates für virtuelle Appliances zur Verwendung mit einem CD-ROM-Laufwerk

Sie können Ihre virtuelle Appliance von einer ISO-Datei aktualisieren, die die Appliance vom virtuellen CD-ROM-Laufwerk liest. Dies ist die bevorzugte Methode.

Sie laden die ISO-Datei herunter und legen die primäre Appliance fest, um diese Datei zum Upgrade Ihrer Appliance zu verwenden.

Voraussetzungen

- Sichern Sie Ihre vorhandene vRealize Automation-Umgebung.
- Vergewissern Sie sich, dass alle in Ihrem Upgrade verwendeten CD-ROM-Laufwerke aktiviert sind, bevor Sie eine vRealize Automation-Appliance aktualisieren. Weitere Informationen zum Hinzufügen eines CD-ROM-Laufwerks zu einer virtuellen Maschine im vSphere-Client finden Sie in der vSphere-Dokumentation.

Verfahren

- 1 Laden Sie die ISO-Datei für das Update-Repository herunter.
 - a Starten Sie einen Browser und navigieren Sie zur [vRealize Automation-Produktseite](#) auf www.vmware.com.
 - b Klicken Sie auf **vRealize Automation-Downloads**, um zur Downloadseite von VMware zu gelangen.
 - c Laden Sie die entsprechende Datei herunter.
- 2 Suchen Sie die heruntergeladene Datei auf Ihrem System, um sicherzustellen, dass die Dateigröße der Größe der Datei auf der Downloadseite von VMware entspricht. Überprüfen Sie die Integrität Ihrer heruntergeladenen Datei mithilfe des Prüfsummenwerts, der auf der Downloadseite angegeben ist. Weitere Informationen finden Sie unter den Links unten auf der Downloadseite von VMware.
- 3 Vergewissern Sie sich, dass die primäre virtuelle Appliance eingeschaltet ist.
- 4 Verbinden Sie das CD-ROM-Laufwerk für die primäre virtuelle Appliance mit der ISO-Datei, die Sie heruntergeladen haben.
- 5 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 6 Klicken Sie auf die Registerkarte **Update**.
- 7 Klicken Sie auf **Einstellungen**.
- 8 Wählen Sie unter „Update-Repository“ die Option **CD-ROM-Updates verwenden** aus.
- 9 Klicken Sie auf **Einstellungen speichern**.

Aktualisieren der vRealize Automation -Appliance

Nachdem Sie die Upgrade-Voraussetzungen erfüllt und das Update der virtuellen Appliance heruntergeladen haben, führen Sie ein Update der vRealize Automation 6.2.5-Appliance auf 7.4 durch. Sie konfigurieren auch einige Einstellungen für die primäre vRealize Automation-Appliance neu.

Nach dem Upgrade der primären vRealize Automation-Appliance führen Sie das Upgrade der übrigen Knoten in Ihrer Umgebung in der nachstehenden Reihenfolge durch:

- 1 Jede sekundäre vRealize Automation-Appliance
- 2 IaaS-Website

- 3 IaaS-Manager Service
- 4 IaaS-DEM
- 5 IaaS-Agent
- 6 Aktualisieren oder migrieren Sie jede externe vRealize Orchestrator-Instanz

Installieren des Updates auf der vRealize Automation -Appliance

Sie installieren das vRealize Automation-Update auf der vRealize Automation 6.2.5-Appliance und konfigurieren die Appliance-Einstellungen.

Der Support für eine externe PostgreSQL-Datenbank wird ab vRealize Automation 7.1 eingestellt. Der Upgrade-Prozess führt die Daten aus einer vorhandenen externen PostgreSQL-Datenbank und der internen PostgreSQL-Datenbank zusammen, die Teil der vRealize Automation-Appliance ist.

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>.

Die Verwaltungskonsole dürfen Sie nicht schließen, während Sie das Update installieren.

Wenn beim Upgrade-Vorgang Probleme auftreten, erhalten Sie im Abschnitt [Fehlerbehebung bei vRealize Automation-Upgrades](#) Unterstützung.

Voraussetzungen

- Vergewissern Sie sich, dass Sie eine Downloadmethode gewählt und das Update heruntergeladen haben. Siehe [Herunterladen von Updates für vRealize Automation-Appliances](#).
- Informationen zu verteilten Hochverfügbarkeitsbereitstellungen finden Sie unter [Sichern Ihrer vorhandenen vRealize Automation 6.2.5-Umgebung](#).
- Wenn die Bereitstellung Lastausgleichsdienste verwendet, stellen Sie sicher, dass der Datenverkehr nur an den primären Knoten geleitet wird und dass die Systemüberwachung deaktiviert ist.
- Wenn der Katalog „Gemeinsame Komponenten“ in Ihrer Umgebung installiert ist, müssen Sie die Komponente vor dem Upgrade deinstallieren. Weitere Informationen finden Sie im *Installationshandbuch für den Katalog „Gemeinsame Komponenten“*. Wenn dieses Handbuch nicht verfügbar ist, verwenden Sie das alternative Verfahren in der [Checkliste für das Upgrade von vRealize Automation](#).
- Stellen Sie sicher, dass die jdbc:postgresql-Datenbankverbindung auf die externe IP-Adresse des PostgreSQL-Knotens verweist.
 - a Öffnen Sie in jeder vRealize Automation-Appliance eine neue Eingabeaufforderung.
 - b Navigieren Sie zum Verzeichnis `/etc/vcac/server.xml` und sichern Sie die Datei `server.xml`.
 - c Öffnen Sie die Datei `server.xml`.
 - d Bearbeiten Sie bei Bedarf den Eintrag „jdbc:posgresql“ der Datei „server.xml“, der auf die PostgreSQL-Datenbank verweist, und legen Sie den Verweis auf die externe IP-Adresse des PostgreSQL-Master-Knotens für externes PostgreSQL oder der primären virtuellen Appliance für eingebettetes PostgreSQL fest.

Beispiel: `jdbc:postgresql://198.15.100.60:5432/vcac`

- Vergewissern Sie sich, dass alle gespeicherten und laufenden Anforderungen erfolgreich abgeschlossen wurden, bevor Sie das Upgrade durchführen.

Verfahren

- 1 Öffnen Sie die Verwaltungskonsole der vRealize Automation-Appliance.
 - a Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
 - b Melden Sie sich mit dem beim Bereitstellen der Appliance eingegebenen Benutzernamen **root** und dem zugehörigen Kennwort an.
- 2 Klicken Sie auf **Dienste** und stellen Sie sicher, dass alle Dienste außer „iaas-service“ als REGISTRIERT aufgeführt sind.
- 3 Wählen Sie **Update > Einstellungen** aus.
- 4 Wählen Sie eine der folgenden Optionen aus:
 - **Standard-Repository verwenden.**
 - **CD-ROM-Updates verwenden**
- 5 Klicken Sie auf **Einstellungen speichern**.
- 6 Wählen Sie **Status** aus.
- 7 Klicken Sie auf **Nach Updates suchen**, um zu überprüfen, ob ein Update verfügbar ist.
- 8 (Optional) Klicken Sie für Instanzen der vRealize Automation-Appliance im Bereich „Appliance-Version“ auf **Details**, um Informationen zum Speicherort von Versionshinweisen anzuzeigen.
- 9 Klicken Sie auf **Updates installieren**.
- 10 Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die besagt, dass das Update ausgeführt wird.
- 11 (Optional) Wenn Sie die Größe der Festplatte 1 nicht manuell in 50 GB geändert haben, führen Sie die folgenden Schritte durch.
 - a Wenn Sie aufgefordert werden, die virtuelle Appliance neu zu starten, klicken Sie auf **System** und dann auf **Neu starten**.

Während des Neustarts wird der für das Update erforderliche Speicherplatz angepasst.
 - b Nachdem das System neu gestartet wurde, melden Sie sich erneut bei der Verwaltungskonsole der vRealize Automation-Appliance an, stellen Sie sicher, dass alle Dienste außer „iaas-service“ als REGISTRIERT aufgeführt sind, und wählen Sie **Aktualisieren > Status** aus.
 - c Klicken Sie auf **Nach Updates suchen** und **Updates installieren**.
- 12 Öffnen Sie die folgenden Protokolldateien, um den Upgrade-Vorgang anzuzeigen.
 - `/opt/vmware/var/log/vami/updatecli.log`

- /opt/vmware/var/log/vami/vami.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

Wenn Sie sich während des Upgrade-Prozesses abmelden und anschließend wieder anmelden, bevor das Upgrade abgeschlossen ist, wird der Fortschritt des Updates in der Protokolldatei angezeigt. In der Datei `updatecli.log` werden möglicherweise Informationen zu der Version von vRealize Automation angezeigt, für die Sie das Upgrade durchführen. Diese angezeigte Version wird später im Upgrade-Vorgang in die entsprechende Version geändert.

Die benötigte Zeit für das Abschließen des Updates hängt von Ihrer Umgebung ab.

- 13** Klicken Sie in der Appliance-Verwaltungskonsole auf **Telemetrie**. Lesen Sie den Hinweis über die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) und wählen Sie aus, ob Sie an dem Programm teilnehmen möchten.

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>.

Weitere Informationen zum Programm zur Verbesserung der Kundenzufriedenheit finden Sie unter [Anmelden beim bzw. Abmelden vom VMware Programm zur Verbesserung der Kundenzufriedenheit für vRealize Automation](#).

Nächste Schritte

[Ihr Single Sign-On-Kennwort für VMware Identity Manager aktualisieren](#).

Ihr Single Sign-On-Kennwort für VMware Identity Manager aktualisieren

Nach der Installation der Updates müssen Sie das Single Sign-On-Kennwort für VMware Identity Manager aktualisieren.

VMware Identity Manager ersetzt die SSO-Komponenten für Identity Appliance und vSphere.

Verfahren

- 1 Melden Sie sich von der Verwaltungskonsole der vRealize Automation-Appliance ab, schließen Sie den Browser, öffnen Sie ihn erneut und melden Sie sich erneut an.
- 2 Wählen Sie **vRA-Einstellungen > SSO** aus.
- 3 Geben Sie ein neues VMware Identity Manager Kennwort ein und klicken Sie auf **Einstellungen speichern**.

Verwenden Sie keine einfachen Kennwörter. Sie können problemlos die angezeigte Fehlermeldung SSO-Server ist nicht verbunden. Es kann einige Minuten dauern, bis der Dienst neu gestartet wird..

Das Kennwort wurde akzeptiert.

Für eine Bereitstellung mit Hochverfügbarkeit wird das Kennwort auf den ersten Knoten der vRealize Automation-Appliance angewendet und an alle sekundären Knoten der vRealize Automation-Appliance weitergegeben.

- 4 Starten Sie die virtuelle Appliance neu.
 - a Klicken Sie auf die Registerkarte **System**.
 - b Klicken Sie auf **Neustart** und bestätigen Sie Ihre Auswahl.
- 5 Stellen Sie sicher, dass alle Dienste ausgeführt werden.
 - a Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance an.
 - b Klicken Sie auf die Registerkarte **Dienste** auf der Konsole.
 - c Klicken Sie auf die Registerkarte **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Es sollten mindestens 35 Dienste angezeigt werden.

- 6 Stellen Sie sicher, dass alle Dienste außer „iaas-service“ registriert sind.

Der Versionsverwaltungs-Dienst startet erst nach Eingabe eines vRealize Code Stream-Lizenzschlüssels.

Nächste Schritte

[Aktualisieren des Lizenzschlüssels](#).

Aktualisieren des Lizenzschlüssels

Sie müssen den Lizenzschlüssel aktualisieren, um die neueste Version der vRealize Automation-Appliance zu verwenden.

Verfahren

- 1 Wechseln Sie zur Verwaltungskonsole für Ihre virtuelle Appliance unter Verwendung des vollqualifizierten Domännennamens „https://va-hostname.domain.name:5480“.
- 2 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance eingegeben haben.
- 3 Wählen Sie **vRA-Einstellungen > Lizenzierung** aus.

Wenn die Registerkarte **Lizenzierung** nicht verfügbar ist, führen Sie die folgenden Schritte aus und wiederholen Sie den Vorgang.

 - a Melden Sie sich von der Managementkonsole ab.
 - b Löschen Sie den Cache Ihres Browsers.
- 4 Geben Sie den neuen Lizenzschlüssel in das Textfeld **Neuer Lizenzschlüssel** ein.

Endpoints und Kontingente werden gemäß Ihrer Endbenutzerlizenzvereinbarung (EULA) markiert.
- 5 Klicken Sie auf **Schlüssel senden**.

Nächste Schritte

[Migrieren von Identitätsquellen auf VMware Identity Manager.](#)

Migrieren von Identitätsquellen auf VMware Identity Manager

Bei einem Upgrade von Version 6.2.5 auf die aktuelle Version von vRealize Automation müssen Sie die Identitätsquellen migrieren.

Sehen Sie sich bei Bedarf den Snapshot Ihrer Informationen zur Mandantenkonfiguration von Version 6.2.5 an.

Hinweis Nach der Migration der Identitätsquellen müssen Benutzer von vRealize Code Stream die vRealize Code Stream-Rollen manuell neu zuweisen.

Verfahren

1 Erstellen eines lokalen Benutzerkontos für Ihre Mandanten

Sie müssen einen Mandanten mit einem lokalen Benutzerkonto einrichten und dem lokalen Benutzerkonto Mandantenadministratorrechte zuweisen.

2 Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link

Um Ihre Benutzer und Gruppen mithilfe der Verzeichnisverwaltung direkt in vRealize Automation zu importieren, müssen Sie eine Verbindung zu Ihrem Active Directory-Link herstellen.

3 Migrieren von benutzerdefinierten Gruppen zum VMware Identity Manager des Ziels

Sie müssen alle benutzerdefinierte Gruppen aus der Quellumgebung zum VMware Identity Manager (vIDM) in der Zielbereitstellung migrieren.

4 Migrieren von mehreren Mandanten- und IaaS-Administratoren

Für jeden vRealize Automation-Mandanten mit Mandanten- oder IaaS-Administratoren müssen Sie jeden Administrator manuell löschen und wiederherstellen.

Erstellen eines lokalen Benutzerkontos für Ihre Mandanten

Sie müssen einen Mandanten mit einem lokalen Benutzerkonto einrichten und dem lokalen Benutzerkonto Mandantenadministratorrechte zuweisen.

Wiederholen Sie dieses Verfahren für jeden Ihrer Mandanten.

Voraussetzungen

Vergewissern Sie sich, dass Sie ein neues Kennwort für VMware Identity Manager festgelegt haben. Siehe [Ihr Single Sign-On-Kennwort für VMware Identity Manager aktualisieren](#).

Verfahren

- 1 Melden Sie sich an der vRealize Automation-Konsole mit dem standardmäßigen Systemadministrator-Benutzernamen **administrator** und dem zugehörigen Kennwort an.

Das Verzeichnis der Konsole ist `https://vra-appliance/vcac/`.

2 Klicken Sie auf Ihren Mandanten.

Klicken Sie beispielsweise für den Standardmandanten auf **vsphere.local**.

3 Wählen Sie die Registerkarte **Lokale Benutzer** aus.

4 Klicken Sie auf **Neu**.

5 Erstellen Sie ein lokales Benutzerkonto.

Diesem Benutzer werden Sie anschließend die Mandantenadministratorrolle zuweisen. Stellen Sie sicher, dass der lokale Benutzername im Active Directory „vsphere.local“ eindeutig ist.

6 Klicken Sie auf **OK**.

7 Klicken Sie auf **Administratoren**.

8 Geben Sie den lokalen Benutzernamen im Suchfeld **Mandantenadministratoren** ein und drücken Sie die Eingabetaste.

9 Klicken Sie auf **Fertig stellen**.

10 Melden Sie sich von der Konsole ab.

Nächste Schritte

[Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link.](#)

Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link

Um Ihre Benutzer und Gruppen mithilfe der Verzeichnisverwaltung direkt in vRealize Automation zu importieren, müssen Sie eine Verbindung zu Ihrem Active Directory-Link herstellen.

Führen Sie dieses Verfahren für jeden Ihrer Mandanten durch.

Voraussetzungen

Überprüfen Sie, ob Sie über Zugriffsberechtigungen für das Active Directory verfügen.

Verfahren

1 Melden Sie sich wie folgt an der vRealize Automation-Konsole an:

`https://vra-appliance/vcac/org/tenant_name`.

2 Wählen Sie **Administration > Verzeichnisverwaltung > Verzeichnisse** aus.

3 Klicken Sie auf **Verzeichnis hinzufügen** und wählen Sie **Active Directory über LDAP/IWA hinzufügen** aus.

4 Geben Sie Ihre Active Directory-Kontoeinstellungen ein.

◆ Nicht-natives Active Directory

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie „Active Directory über LDAP“ aus, wenn ein nicht-natives Active Directory verwendet wird.
Dieses Verzeichnis unterstützt DNS-Dienste	Deaktivieren Sie diese Option.
Basis-DN	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: cn=users,dc=rainpole,dc=local.
Bind-DN	Geben Sie den vollständigen definierten Namen (DN, Distinguished Name), einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Beispiel: cn=config_admin infra,cn=users,dc=rainpole,dc=local.
Bind-DN-Kennwort	Geben Sie das Active Directory-Kennwort für das Konto ein, das nach Benutzern suchen kann.

◆ Natives Active Directory

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie „Active Directory“ (Integrierte Windows-Authentifizierung) aus, wenn „Natives Active Directory“ verwendet wird.
Domänenname	Geben Sie den Namen der Domäne ein, der beigetreten werden soll.
Benutzername des Domänenadministrators	Geben Sie den Benutzernamen für den Domänenadministrator ein.
Kennwort des Domänenadministrators	Geben Sie das Kennwort für das Konto des Domänenadministrators ein.
Bind-Benutzer-UPN	Geben Sie als Benutzernamen die E-Mail-Adresse des Benutzers ein, der die Domäne authentifizieren kann.
Bind-DN-Kennwort	Geben Sie das Kennwort des Active Directory-Bind-Kontos für das Konto ein, das nach Benutzern suchen kann.

5 Klicken Sie auf **Verbindung testen**, um die Verbindung zum konfigurierten Verzeichnis zu testen.

6 Klicken Sie auf **Speichern und weiter**.

Die Seite **Domänen auswählen** mit der Liste der Domänen wird angezeigt.

7 Übernehmen Sie die Einstellung für die Standarddomäne und klicken Sie auf **Weiter**.

8 Überprüfen Sie, ob die Attributnamen den richtigen Active Directory-Attributen zugeordnet sind, und klicken Sie auf **Weiter**.

- 9 Wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen.
 - a Klicken Sie auf das Symbol **Neu**.
 - b Geben Sie die Benutzerdomäne ein und klicken Sie auf **Gruppen suchen**.
Geben Sie beispielsweise **dc=vcac,dc=local** ein.
 - c Um die Gruppen zur Synchronisierung zu wählen, klicken Sie auf **Auswählen** und **Weiter**.
 - d Wählen Sie auf der Seite **Benutzer auswählen** die Benutzer aus, die synchronisiert werden sollen, und klicken Sie auf **Weiter**.
- 10 Überprüfen Sie die Benutzer und Gruppen, die mit dem Verzeichnis synchronisiert werden, und klicken Sie auf **Verzeichnis synchronisieren**.

Für die Verzeichnissynchronisierung wird einige Zeit benötigt. Der Prozess wird im Hintergrund ausgeführt.
- 11 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus und klicken Sie auf Ihren neuen Identitätsanbieter.

Beispiel: **WorkspaceIDP__1**.
- 12 Führen Sie einen Bildlauf bis zum Ende der Seite durch und aktualisieren Sie den Wert für die Eigenschaft „IdP-Hostname“, um auf den FQDN für den vRealize Automation-Lastausgleichsdienst zu zeigen.
- 13 Klicken Sie auf **Speichern**.
- 14 Wiederholen Sie die Schritte 11-13 für jeden Mandanten und Identitätsanbieter.
- 15 Nach dem Upgrade aller vRealize Automation-Knoten melden Sie sich bei jedem Mandanten an und wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter**.

Jedem Identitätsanbieter sind alle vRealize Automation-Konnektoren hinzugefügt worden.

Wenn Ihre Bereitstellung beispielsweise über zwei vRealize Automation-Appliances verfügt, weist der Identitätsanbieter zwei zugeordnete Konnektoren auf.

Migrieren von benutzerdefinierten Gruppen zum VMware Identity Manager des Ziels

Sie müssen alle benutzerdefinierte Gruppen aus der Quellumgebung zum VMware Identity Manager (vIDM) in der Zielbereitstellung migrieren.

Führen Sie dieses Verfahren durch, um benutzerdefinierte Gruppen zu migrieren.

Voraussetzungen

- [Erstellen eines lokalen Benutzerkontos für Ihre Mandanten](#).
- Stellen Sie sicher, dass der Horizon-Workspace-Dienst auf der virtuellen vRealize Automation-Appliance ausgeführt wird.

Verfahren

- 1 Starten Sie eine SSH-Sitzung auf der virtuellen vRealize Automation-Appliance.

- 2 Melden Sie sich an der Eingabeaufforderung als **root** mit dem Kennwort an, das Sie beim Installieren der virtuellen vRealize Automation-Appliance erstellt haben.
- 3 Führen Sie diesen Befehl aus.

```
vcac-config migrate-custom-groups
```

- Eine Meldung ähnlich der folgenden wird angezeigt, wenn die Migration abgeschlossen ist: Die Migration der benutzerdefinierten Gruppen wurde erfolgreich abgeschlossen!
- Eine Meldung ähnlich der folgenden wird angezeigt, wenn sich in der Quellumgebung keine benutzerdefinierten Gruppen befinden: In der vRA-Datenbank wurden keine benutzerdefinierten Gruppen gefunden. Migrationsvorgang wird übersprungen.

Hinweis Wenn die Migration benutzerdefinierter Gruppen fehlschlägt, finden Sie Informationen hierzu in der Protokolldatei unter `/var/log/vmware/vcac/vcac-config.log`.

Migrieren von mehreren Mandanten- und IaaS-Administratoren

Für jeden vRealize Automation-Mandanten mit Mandanten- oder IaaS-Administratoren müssen Sie jeden Administrator manuell löschen und wiederherstellen.

Führen Sie die folgenden Schritte für jeden Mandanten in der vRealize Automation-Konsole aus.

Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole auf der aktualisierten virtuellen Appliance an.

- 1 Öffnen Sie die vRealize Automation-Konsole auf der aktualisierten virtuellen Appliance mithilfe des vollqualifizierten Domännennamens, `https://va-hostname.domain_name/vcac`.

Für eine verteilte Umgebung öffnen Sie die Konsole auf der virtuellen Master-Appliance.

- 2 Wählen Sie die Domäne **vsphere.local** aus.
- 3 Melden Sie sich mit dem beim Bereitstellen der virtuellen Appliance eingegebenen Benutzernamen **Administrator** und dem zugehörigen Kennwort an.

Verfahren

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf einen Mandantennamen.
- 3 Klicken Sie auf **Administratoren**.
- 4 Erstellen Sie eine Liste mit den Namen und Benutzernamen der einzelnen Mandanten- und IaaS-Administratoren.
- 5 Zeigen Sie auf jeden Administrator und klicken Sie so lange auf das Symbol „Löschen“ (✘), bis Sie alle Administratoren gelöscht haben.
- 6 Klicken Sie auf **Fertig stellen**.
- 7 Klicken Sie auf der Seite „Mandanten“ erneut auf den Namen des Mandanten.

- 8 Klicken Sie auf **Administratoren**.
- 9 Geben Sie die Namen aller gelöschten Benutzer in das entsprechende Suchfeld ein und drücken Sie die Eingabetaste.
- 10 Klicken Sie in den Suchergebnissen auf den Namen des jeweiligen Benutzers, um ihn wieder als Administrator hinzuzufügen.

Wenn Sie fertig sind, stimmen die Liste der Mandanten- und IaaS-Administratoren und die Liste der gelöschten Administratoren überein.

- 11 Klicken Sie auf **Fertig stellen**.

Nächste Schritte

Führen Sie ein Upgrade der sekundären Appliances durch. Siehe [Installieren des Updates auf zusätzlichen vRealize Automation-Appliances](#).

Installieren des Updates auf zusätzlichen vRealize Automation -Appliances

In einer Hochverfügbarkeitsumgebung ist die virtuelle Master-Appliance der Knoten, der die eingebettete PostgreSQL-Datenbank im Master-Modus ausführt. Die anderen Knoten in der Umgebung führen die eingebettete PostgreSQL-Datenbank im Replikatmodus aus. Während des Upgrades sind für das Replikat einer virtuellen 6.2.5-Appliance keine Datenbankänderungen erforderlich.

Die Verwaltungskonsole dürfen Sie nicht schließen, während Sie das Update installieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Updates der virtuellen Appliance heruntergeladen haben. Siehe [Herunterladen von Updates für vRealize Automation-Appliances](#).
- Stellen Sie sicher, dass die jdbc:postgresql-Datenbankverbindung auf die externe IP-Adresse des PostgreSQL-Knotens verweist.
 - a Öffnen Sie auf der vRealize Automation-Appliance eine neue Eingabeaufforderung.
 - b Navigieren Sie zu `/etc/vcac/server.xml` und sichern Sie die `server.xml`-Datei.
 - c Öffnen Sie die Datei „`server.xml`“.
 - d Bearbeiten Sie bei Bedarf den Eintrag „`jdbc:postgresql`“ in der Datei `server.xml`, um die PostgreSQL-Datenbank anzugeben, die Sie verwenden möchten.
 - Geben Sie für eine externe PostgreSQL-Datenbank die externe IP-Adresse des PostgreSQL-Master-Knotens ein.
 - Geben Sie die IP-Adresse der virtuellen Master-Appliance für die eingebettete PostgreSQL-Datenbank ein.

Beispiel: `jdbc:postgresql://198.15.100.60:5432/vcac`

Verfahren

- 1 Öffnen Sie die Verwaltungskonsole der vRealize Automation-Appliance für das Upgrade.
 - a Melden Sie sich auf jeder sekundären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
 - b Melden Sie sich mit dem beim Bereitstellen der Appliance eingegebenen Benutzernamen **root** und dem zugehörigen Kennwort an.
 - c Klicken Sie auf **Aktualisieren**.
- 2 Klicken Sie auf **Einstellungen**.
- 3 Geben Sie im Abschnitt „Update-Repository“ an, ob die Updates aus einem VMware-Repository oder von einer CD-ROM heruntergeladen werden sollen.
- 4 Klicken Sie auf **Status**.
- 5 Klicken Sie auf **Nach Updates suchen**, um zu überprüfen, ob ein Update verfügbar ist.
- 6 Klicken Sie auf **Updates installieren**.
- 7 Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die besagt, dass das Update ausgeführt wird.

- 8 (Optional) Wenn Sie die Größe der Festplatte 1 nicht manuell von 1 GB in 50 GB geändert haben, führen Sie die folgenden Schritte durch.
 - a Wenn Sie aufgefordert werden, die virtuelle Appliance neu zu starten, klicken Sie auf **System** und dann auf **Neu starten**.

Während des Neustarts wird der für das Update erforderliche Speicherplatz auf der Festplatte 1 angepasst.
 - b Melden Sie sich nach dem Neustart des Systems erneut an der vRealize Automation-Appliance-Verwaltungskonsole an und wählen Sie **Aktualisieren > Status** aus.
 - c Klicken Sie auf **Nach Updates suchen** und **Updates installieren**.
- 9 Um sicherzustellen, dass das Upgrade erfolgreich verläuft, öffnen Sie die Protokolldateien.
 - /opt/vmware/var/log/vami/vami.log
 - /opt/vmware/var/log/vami/updatecli.log
 - /var/log/vmware/horizon/horizon.log
 - /var/log/bootstrap/*.log

Wenn Sie sich während des Upgrade-Prozesses abmelden und anschließend wieder anmelden, wird der Fortschritt des Updates in der Protokolldatei /opt/vmware/var/log/vami/updatecli.log angezeigt.

Die benötigte Zeit für das Abschließen des Updates hängt von Ihrer Umgebung ab.

- 10 Wenn das Update abgeschlossen ist, melden Sie sich von der vRealize Automation-Appliance-Verwaltungskonsole ab, deaktivieren Sie den Webbrowser-Cache und melden Sie sich bei der vRealize Automation-Appliance-Verwaltungskonsole an.
- 11 Starten Sie die virtuelle Appliance neu.
 - a Klicken Sie auf **System**.
 - b Klicken Sie auf **Neustart** und bestätigen Sie Ihre Auswahl.
- 12 Melden Sie sich nach dem Neustart der virtuellen Appliance bei der Replikat-vRealize Automation-Appliance-Verwaltungskonsole an.
- 13 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 14 Geben Sie den Master-vRealize Automation-Appliance-Benutzernamen und das zugehörige Kennwort ein.
- 15 Klicken Sie auf **Cluster beitreten**.
- 16 Klicken Sie auf **Dienste** und stellen Sie sicher, dass alle Dienste außer „iaas-service“ als REGISTRIERT aufgeführt sind.

Nächste Schritte

[Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation.](#)

Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation

Nach dem Upgrade von vRealize Automation 6.2.5 auf 7.4 aktualisiert ein Systemadministrator die IaaS-Serverkomponenten einschließlich der Microsoft SQL Server-Datenbank.

Sie können die IaaS-Serverkomponenten auf zwei Arten installieren.

- Verwenden Sie das automatisierte IaaS-Upgrade-Shell-Skript.
- Verwenden Sie die ausführbare Datei des IaaS-Installationsprogramms für vRealize Automation 7.4.

Wenn der Katalog „Gemeinsame Komponenten“ installiert ist, müssen Sie die Komponente vor dem Upgrade deinstallieren. Nach Abschluss des Upgrades können Sie die Komponente mit der entsprechenden Version erneut installieren. Weitere Informationen finden Sie im *Installationshandbuch für den Katalog „Gemeinsame Komponenten“*. Wenn dieses Handbuch nicht verfügbar ist, wenden Sie das alternative Verfahren in [Checkliste für das Upgrade von vRealize Automation](#) an.

Upgrade der IaaS-Komponenten mit dem Upgrade-Shell-Skript

Aktualisieren Sie die IaaS-Komponenten mithilfe des Upgrade-Shell-Skripts, nachdem Sie das Update für alle vRealize Automation 6.2.5-Appliances auf 7.4. durchgeführt haben.

Die aktualisierte primäre oder Master-vRealize Automation-Appliance enthält ein Shell-Skript, das Sie zum Upgrade jedes IaaS-Knotens und jeder Komponente verwenden.

Sie können das Upgrade-Skript ausführen, indem Sie die vSphere-Konsole für die virtuelle Maschine oder eine SSH-Konsolensitzung verwenden. Wenn Sie die vSphere-Konsole verwenden, vermeiden Sie temporäre Probleme bei der Netzwerkkonnektivität, die zur fehlerhaften Ausführung des Skripts führen können.

Wenn Sie das Skript beenden, während eine Komponente aktualisiert wird, wird das Skript weiterhin ausgeführt, bis das Upgrade der Komponente abgeschlossen ist. Wenn einige Komponenten auf dem Knoten nicht aktualisiert werden, müssen Sie das Skript erneut ausführen.

Nach Abschluss des Upgrades können Sie das Upgrade-Ergebnis überprüfen, indem Sie die Upgrade-Protokolldatei im Verzeichnis `/usr/lib/vcac/tools/upgrade/upgrade.log` öffnen.

Voraussetzungen

- Vergewissern Sie sich, dass alle vRealize Automation-Appliances erfolgreich aktualisiert wurden.
- Wenn Sie einen IaaS-Server neu starten, nachdem Sie alle vRealize Automation-Appliances aktualisiert haben, müssen Sie die IaaS-Windows-Dienste beenden. Bevor Sie die IaaS-Komponenten aktualisieren, beenden Sie alle IaaS-Windows-Dienste mit Ausnahme des Management-Agent-Dienstes auf dem Server.
- Bevor Sie das Upgrade-Shell-Skript auf dem Master- bzw. dem primären vRealize Automation-Appliance-Knoten ausführen, stellen Sie sicher, dass jeder Dienst registriert ist.
 - a Wechseln Sie zur Appliance-Verwaltungskonsole für Ihre virtuelle Appliance unter Verwendung des vollqualifizierten Domännennamens: `https://va-hostname.domain.name:5480`.
 - b Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance eingegeben haben.
 - c Klicken Sie auf **Dienste**.
 - d Stellen Sie sicher, dass alle Dienste außer dem IaaS-Dienst registriert sind.
- Führen Sie ein Upgrade des Management-Agents auf jeder virtuellen vRealize Automation-IaaS-Maschine durch.
 - a Öffnen Sie einen Browser und wechseln Sie zur VMware vRealize Automation-IaaS-Installationsseite auf der vRealize Automation-Appliance mit dem vollqualifizierten Domännennamen: `https://virtual_appliance_host:5480/installer`.
 - b Klicken Sie auf das **Management-Agent-Installationsprogramm**.
Das Installationsprogramm wird standardmäßig in den Downloads-Ordner heruntergeladen.
 - c Melden Sie sich bei jeder virtuellen vRealize Automation-IaaS-Maschine an und führen Sie das Upgrade des Management-Agent mit dem **Installationsprogramm des Management-Agents** durch.
- Stellen Sie sicher, dass der primäre IaaS-Websiteknoten, auf dem die Model Manager-Daten installiert sind, über JAVA SE Runtime Environment 8, 64 Bit, Update 161 oder höher verfügt. Nach der Installation von Java müssen Sie die Umgebungsvariable `JAVA_HOME` auf die neue Version aktualisieren.

- Melden Sie sich bei jedem IaaS-Websiteknoten an und stellen Sie sicher, dass das Erstellungsdatum für die Datei `web.config` vor dem Änderungsdatum liegt. Wenn das Erstellungsdatum für die Datei `web.config` mit dem Änderungsdatum übereinstimmt oder dahinter liegt, führen Sie den Vorgang in [Upgrade für die IaaS-Website-Komponente schlägt fehl](#) aus.
- Um sicherzustellen, dass jeder IaaS-Knoten über einen aktualisierten IaaS-Management-Agent verfügt, führen Sie diese Schritte auf jedem IaaS-Knoten durch.
 - a Melden Sie sich bei der Verwaltungskonsole der vRealize Automation-Appliance an.
 - b Wählen Sie **vRA-Einstellungen > Cluster** aus.
 - c Erweitern Sie die Liste aller installierten Komponenten für jeden IaaS-Knoten und suchen Sie den IaaS-Management-Agent.
 - d Stellen Sie sicher, dass der Management-Agent auf die aktuelle Version aktualisiert wurde.
- Vergewissern Sie sich, dass Sie auf die IaaS-Microsoft SQL Server-Datenbank zugreifen können, falls Sie ein Rollback durchführen müssen.
- Löschen Sie alle verwaisten IaaS-Knoten. Siehe [Löschen von verwaisten Knoten in vRealize Automation](#).
- Vergewissern Sie sich, dass Snapshots der IaaS-Servers in Ihrer Bereitstellung verfügbar sind.
Wenn das Upgrade nicht erfolgreich ist, stellen Sie den Snapshot und das Datenbank-Update wiederher und versuchen Sie es erneut.

Verfahren

- 1 Öffnen Sie eine neue Konsolensitzung auf dem primären oder Master-vRealize Automation-Appliance-Knoten und melden Sie sich mit dem Root-Konto an.
Wenn Sie das Upgrade-Skript über SSH ausführen möchten, öffnen Sie eine SSH-Konsolensitzung.
- 2 Wechseln Sie zum Verzeichnis `/usr/lib/vcac/tools/upgrade/`.
- 3 Führen Sie an der Eingabeaufforderung folgenden Befehl aus, um die Datei `upgrade.properties` zu erstellen.
`./generate_properties`
- 4 Öffnen Sie die `upgrade.properties`-Datei und geben Sie alle Werte ein.

In dieser Tabelle finden Sie die Werte, die je nach Umgebung variieren. So sind beispielsweise an einem Knoten, der einen DEM Worker oder Orchestrator enthält, DEM-Anmeldedaten erforderlich.

Erforderlicher Wert	Beschreibung	Format der Anmeldedaten	Beispielwert
<code>web_username</code>	Benutzername für den primären Webknoten. Nur einmal erforderlich.	Domäne\Benutzer	<code>iaasDomain\webuser</code>
<code>web_password</code>	Kennwort für den primären Webknoten. Nur einmal erforderlich.	Kennwort	<code>pa\$\$w0rd!</code>

Erforderlicher Wert	Beschreibung	Format der Anmeldedaten	Beispielwert
dem_username	Benutzername für den DEM Worker oder DEM Orchestrator. Für jeden Knoten erforderlich, auf dem eine DEM-Komponente installiert ist.	Domäne\Benutzer	iaasDomain\demuser
dem_password	Kennwort für den DEM Worker oder DEM Orchestrator. Für jeden Knoten erforderlich, auf dem eine DEM-Komponente installiert ist.	Kennwort	pa\$\$w0rd!
agent_username	Benutzername für einen Agent, z. B. vSphere-Agent. Für jeden Knoten erforderlich, auf dem eine Agent-Komponente installiert ist.	Domäne\Benutzer	iaasDomain\agent_user
agent_password	Kennwort für einen Agent, z. B. vSphere-Agent. Für jeden Knoten erforderlich, auf dem eine Agent-Komponente installiert ist.	Kennwort	pa\$\$w0rd!
vidm_admin_password	Das VIDM-Administratorkennwort. Nur bei einem Upgrade von vRealize Automation 6.2.5 erforderlich.	vidm_password	pa\$\$w0rd!

Aus Sicherheitsgründen wird die `upgrade.properties`-Datei entfernt, wenn Sie das Upgrade-Shell-Skript ausführen. Die Eigenschaften in der Datei werden mithilfe der Informationen für jede IaaS-Komponente definiert, die über die IaaS-Management-Agents verfügbar sind. Es ist wichtig, dass alle IaaS-Management-Agents vor der Ausführung der `./generate_properties-` oder `./upgrade_from_62x-`Shell-Skripts ordnungsgemäß aktualisiert wurden. Wenn ein IaaS-Management-Agent während des Ausführens des Shell-Skripts ein Problem aufweist, siehe [Beim Update wird kein Upgrade des Management Agents durchgeführt](#). Um die `upgrade.properties`-Datei erneut zu erstellen, wiederholen Sie die Schritte 2 und 3.

- 5 Führen Sie das Upgrade-Skript aus.
 - a Geben Sie in der Eingabeaufforderung `./upgrade_from_62x`.
 - b Drücken Sie die Eingabetaste.

Das Skript zeigt jeden IaaS-Knoten und alle darauf installierten Komponenten an. Vor der Installation des Upgrades prüft das Skript jede Komponente. Wenn die `upgrade.properties`-Datei falsche Werte enthält, schlägt das Skript fehl.

Die Aktualisierung der ersten IaaS-Serverkomponente kann 30 Minuten oder länger dauern. Während des Upgrades wird eine Meldung ähnlich `Upgrading server components for node web1-vra.mycompany.com` angezeigt.

Wenn das Upgrade-Shell-Skript fehlschlägt, sehen Sie sich die Datei `upgrade.log` an.

Sie können das Upgrade-Skript erneut ausführen, nachdem Sie das Problem behoben haben. Erstellen und öffnen Sie die `upgrade.properties`-Datei vor dem Ausführen des Upgrade-Skripts und geben Sie die erforderlichen Werte ein.

- 6 (Optional) Aktivieren Sie das automatische Manager Service-Failover. Siehe [Aktivieren des automatischen Manager Service-Failovers nach einem Upgrade](#).

Nächste Schritte

[Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator-Control Center](#).

Upgrade der IaaS-Komponenten mit dem IaaS-Installationsprogramm

Sie können diese alternative Methode für das Upgrade der IaaS-Komponenten nach dem Upgrade von vRealize Automation 6.2.5 auf 7.4 verwenden.

Herunterladen des IaaS -Installationsprogramms zum Upgrade von IaaS -Komponenten

Laden Sie nach dem Upgrade von vRealize Automation 6.2.5 auf 7.4 das IaaS-Installationsprogramm auf die virtuelle Maschine herunter, auf der die IaaS-Komponenten für das Upgrade installiert sind.

Etwasige Zertifikatswarnungen während dieses Vorgangs können ignoriert werden.

Hinweis Außer für eine passive Sicherungsinstanz des Manager Service muss der Starttyp für alle Dienste während des Upgrades auf „Automatisch“ eingestellt sein. Wenn Sie den Starttyp für die Dienste auf „Manuell“ festlegen, schlägt der Upgrade-Vorgang fehl.

Voraussetzungen

- Stellen Sie sicher, dass Microsoft .NET Framework 4.5.2 oder höher auf der virtuellen IaaS-Zielmaschine für die Installation installiert ist. Das .NET-Installationsprogramm können Sie von der VMware-Seite für die vRealize Automation-IaaS-Installation herunterladen. Wenn Sie .NET auf Version 4.5.2 aktualisieren, nachdem Sie die Dienste heruntergefahren haben, wird die virtuelle Maschine möglicherweise als Teil der Installation neu gestartet. Wenn dies geschieht, müssen Sie alle IaaS-Dienste auf der virtuellen Maschine mit Ausnahme des Management-Agent manuell beenden.
- Achten Sie bei Verwendung von Internet Explorer zum Herunterladen darauf, dass „Verstärkte Sicherheitskonfiguration“ nicht aktiviert ist. Geben Sie `res://iesetup.dll/SoftAdmin.htm` in die Suchleiste ein und drücken Sie die Eingabetaste.
- Melden Sie sich als Administrator bei dem Windows-Server an, auf dem eine oder mehrere der zu aktualisierenden IaaS-Komponenten installiert sind.

Verfahren

- 1 Öffnen Sie einen Webbrowser.
- 2 Geben Sie die URL der VMware-Seite für die vRealize Automation-IaaS-Installation ein.

Beispiel: `https://vcac-va-hostname.domain.name:5480/installer`, wobei `vcac-va-hostname.domain.name` der Name des primären Knotens oder Master-Knotens der vRealize Automation-Appliance ist.

3 Klicken Sie auf **laaS-Installationsprogramm**.

4 Die Installationsdatei `setup__Vcac-va-hostname.domain.name@5480.exe` wird standardmäßig an den Downloads-Ordner gesendet.

Ändern Sie den Dateinamen nicht. Er wird verwendet, um die Installation mit der vRealize Automation-Appliance zu verbinden.

Nächste Schritte

- Wenn Sie über eine eigenständige vRealize Orchestrator-Instanz verfügen, finden Sie weitere Informationen unter [Upgrade einer eigenständigen vRealize Orchestrator Appliance für die Verwendung mit vRealize Automation](#).
- Wenn Sie über einen externen vRealize Orchestrator-Appliance-Cluster verfügen, finden Sie weitere Informationen unter [Upgrade eines externen vRealize Orchestrator Appliance-Clusters für die Verwendung mit vRealize Automation](#).
- Siehe [Upgrade der laaS-Serverkomponenten nach dem Upgrade von vRealize Automation](#).

Upgrade der laaS-Serverkomponenten nach dem Upgrade von vRealize Automation

Nach dem Upgrade von vRealize Automation 6.2.5 auf 7.4 müssen Sie die SQL-Datenbank aktualisieren und alle Systeme konfigurieren, auf denen laaS-Komponenten installiert sind. Sie können diese Schritte für Minimal- und verteilte Installationen befolgen.

Hinweis Das laaS-Installationsprogramm muss sich auf der virtuellen Maschine befinden, die die laaS-Komponenten enthält, für die Sie ein Upgrade durchführen möchten. Sie können das Installationsprogramm nicht von einem externen Standort ausführen, mit Ausnahme der Microsoft SQL-Datenbank, die auch im Remotemodus über den Webknoten aktualisiert werden kann.

Vergewissern Sie sich, dass Snapshots der laaS-Servers in Ihrer Bereitstellung verfügbar sind. Wenn die Aktualisierung fehlschlägt, können Sie den Snapshot wiederherstellen und eine erneute Aktualisierung versuchen.

Führen Sie die Aktualisierung so durch, dass die Dienste in folgender Reihenfolge aktualisiert werden:

1 laaS-Websites

Wenn Sie einen Lastausgleichsdienst verwenden, deaktivieren Sie den Datenverkehr auf allen nicht primären Knoten.

Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren, der einen Website-Dienst ausführt. Beginnen Sie mit dem Server, auf dem die Komponente „Model Manager-Daten“ installiert ist.

Wenn Sie ein manuelles Upgrade der externen Microsoft SQL-Datenbank durchführen, müssen Sie vor der Aktualisierung des Webknotens die externe SQL-Datenbank aktualisieren. Sie können ein Upgrade der externen SQL aus der Ferne über den Webknoten durchführen.

2 Manager Services

Führen Sie zunächst ein Upgrade des aktiven Manager Services und dann des passiven Manager Services durch.

Wenn die SSL-Verschlüsselung auf der SQL-Instanz nicht aktiviert ist, deaktivieren Sie **SSL-Verschlüsselung** im Dialogfeld für die IaaS-Upgrade-Konfiguration.

3 DEM-Orchestrator und -Workers

Aktualisieren Sie alle DEM-Orchestratoren und -Workers. Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren.

4 Agents

Schließen Sie die Aktualisierung auf einem Server ab, bevor Sie den nächsten Server aktualisieren, der einen Agent ausführt.

5 Management-Agent

Wird im Rahmen des Upgradeprozesses aktualisiert.

Wenn Sie verschiedene Dienste auf einem Server verwenden, werden bei der Aktualisierung die Dienste in der richtigen Reihenfolge aktualisiert. Wenn in Ihrer Site z. B. Websitedienste und Manager Services auf dem gleichen Server vorhanden sind, wählen Sie beide für die Aktualisierung aus. Das Aktualisierungs-Installationsprogramm wendet die Updates in der richtigen Reihenfolge an. Sie müssen die Aktualisierung auf einem Server abschließen, bevor Sie mit der Aktualisierung eines anderen Servers beginnen.

Hinweis Wenn Ihre Bereitstellung einen Lastausgleichsdienst verwendet, muss die erste Appliance, die aktualisiert werden soll, mit dem Lastausgleichsdienst verbunden sein. Alle anderen Instanzen von vRealize Automation-Appliance müssen für den Datenverkehr des Lastausgleichsdiensts deaktiviert werden, bevor Sie die Aktualisierung anwenden, um Cachefehler zu vermeiden.

Voraussetzungen

- Sichern Sie Ihre vorhandene vRealize Automation 6.2.5-Umgebung.
- Wenn Sie einen IaaS-Server neu starten, nachdem Sie alle vRealize Automation-Appliances aktualisiert haben, müssen Sie die IaaS-Windows-Dienste beenden. Bevor Sie die IaaS-Komponenten aktualisieren, beenden Sie alle IaaS-Windows-Dienste mit Ausnahme des Management-Agent-Dienstes auf dem Server.
- [Herunterladen des IaaS-Installationsprogramms zum Upgrade von IaaS-Komponenten.](#)
- Stellen Sie sicher, dass Ihr primärer IaaS-Websiteknoten, auf dem die Model Manager-Daten installiert sind, über die richtige Java-Version verfügt. JAVA SE Runtime Environment 8, 64 Bit, Update 161 oder höher muss installiert sein. Aktualisieren Sie die Umgebungsvariable JAVA_HOME nach der Installation von Java auf die neue Version.
- Stellen Sie sicher, dass das Datum der Dateierstellung in der Datei `web.config` vor dem Änderungsdatum liegt. Wenn das Erstellungsdatum für die Datei `web.config` mit dem Änderungsdatum übereinstimmt oder dahinter liegt, führen Sie den Vorgang in [Upgrade für die IaaS-Website-Komponente schlägt fehl](#) aus.

- Wenn Sie von vRealize Automation 6.2.5 aktualisieren und eine externe Microsoft SQL-Datenbank besitzen, müssen Sie über die richtige Management-Agent-Version verfügen. Der Management-Agent auf der externen Datenbank muss Version 7.0 oder höher aufweisen, bevor Sie das IaaS-Website-Upgrade durchführen. Sie können die Version des Management-Agents in der Systemsteuerung Ihrer externen virtuellen SQL-Maschine überprüfen. Wenn der Management-Agent nicht Version 7.0 oder höher aufweist, führen Sie diese Schritte durch, um ihn zu aktualisieren.
 - a Öffnen Sie einen Browser und wechseln Sie zur VMware vRealize Automation-IaaS-Installationsseite auf der vRealize Automation-Appliance-Appliance mit dem vollqualifizierten Domänennamen: `https://virtual_appliance_host:5480/installer`.
 - b Klicken Sie auf das **Management-Agent-Installationsprogramm**.
Das Installationsprogramm wird standardmäßig in den Downloads-Ordner heruntergeladen.
 - c Melden Sie sich bei der externen Datenbank an, führen Sie ein Upgrade des Management-Agents mithilfe des **Management-Agent-Installationsprogramms** durch und starten Sie den Windows Management-Agent-Dienst neu.
- Wenn der Katalog „Gemeinsame Komponenten“ installiert ist, müssen Sie die Komponente vor dem Upgrade deinstallieren. Weitere Informationen finden Sie im *Installationshandbuch für den Katalog „Gemeinsame Komponenten“*. Sie können auch die Schritte unter [Checkliste für das Upgrade von vRealize Automation](#) ausführen.

Verfahren

- 1 Wenn Sie einen Lastausgleichsdienst verwenden, bereiten Sie die Umgebung vor.
 - a Stellen Sie sicher, dass der IaaS-Websiteknoten, der die Model Manager-Daten enthält, für den Datenverkehr des Lastausgleichsdiensts aktiviert ist.
Diesen Knoten erkennen Sie am Vorhandensein des Ordners `vCAC-Ordner\Server\Config-Tool`.
 - b Deaktivieren Sie alle anderen IaaS-Websites und nicht-primären Manager Services für den Datenverkehr des Lastausgleichsdiensts.
- 2 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vrealize-automation-appliance-FQDN@5480.exe` und wählen Sie **Als Administrator ausführen** aus.
- 3 Klicken Sie auf **Weiter**.
- 4 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 5 Geben Sie auf der Anmeldeseite die Administratoranmeldedaten für Ihre aktuelle Bereitstellung ein.
Der Benutzername lautet **root** und das Kennwort ist dasjenige, das Sie bei der Bereitstellung der Appliance eingegeben haben.
- 6 Wählen Sie **Zertifikat akzeptieren** aus.
- 7 Vergewissern Sie sich auf der Seite **Installationstyp**, dass **Aktualisierung** ausgewählt ist.
Wenn **Aktualisierung** nicht ausgewählt ist, sind die Komponenten auf diesem System bereits auf diese Version aktualisiert.

- 8 Klicken Sie auf **Weiter**.
- 9 Konfigurieren Sie die Aktualisierungseinstellungen.

Option	Aktion
Beim Aktualisieren der Model Manager-Daten	<p>Aktivieren Sie das Kontrollkästchen Model Manager-Daten im Abschnitt „vCAC-Server“.</p> <p>Das Kontrollkästchen ist standardmäßig aktiviert. Aktualisieren Sie Model Manager-Daten nur einmal. Wenn Sie eine verteilte Installation aktualisieren und die Versionen der Webserver und der Model Manager-Daten nicht übereinstimmen, funktionieren die Webserver nicht mehr. Wenn das Upgrade der Model Manager-Daten abgeschlossen ist, funktionieren die Webserver wie gewohnt.</p>
Keine Aktualisierung der Model Manager-Daten	<p>Deaktivieren Sie das Kontrollkästchen Model Manager-Daten im Abschnitt „vCAC-Server“.</p>
So behalten Sie angepasste Workflows als neueste Version in den Model Manager-Daten bei	<p>Wenn Sie die Model Manager-Daten aktualisieren, aktivieren Sie das Kontrollkästchen Meine neuesten Workflow-Versionen beibehalten im Abschnitt der Erweiterbarkeits-Workflows.</p> <p>Das Kontrollkästchen ist standardmäßig aktiviert. Angepasste Workflows werden immer beibehalten. Durch Aktivieren des Kontrollkästchens wird nur die Reihenfolge der Versionen bestimmt. Wenn Sie im Model Manager angepasste Workflows haben, wählen Sie diese Option aus, damit der neueste Workflow als die neueste Version nach dem Upgrade erhalten bleibt.</p> <p>Wenn Sie diese Option nicht auswählen, wird die mit vRealize Automation Designer bereitgestellte Version jedes Workflows nach der Aktualisierung die neueste Version. Die neueste Version vor der Aktualisierung wird zur zweitneuesten.</p> <p>Weitere Informationen zu vRealize Automation Designer finden Sie unter <i>Lebenszyklus-Erweiterbarkeit</i>.</p>
Beim Upgrade eines Distributed Execution Manager oder eines Proxy-Agents	<p>Geben Sie die Anmeldedaten für das Administratorkonto im Abschnitt des Dienstkontos ein.</p> <p>Alle Dienste, die Sie aktualisieren, werden unter diesem Konto ausgeführt.</p>
So geben Sie die Microsoft SQL Server-Datenbank an	<p>Wenn Sie die Model Manager-Daten aktualisieren, geben Sie die Namen der Datenbankserver und der Datenbankinstanz in das Textfeld Server ein. Geben Sie einen vollqualifizierten Domänennamen (FQDN) als Datenbankservernamen in das Textfeld Datenbankname ein.</p> <p>Wenn die Datenbank sich an einem anderen als dem Standard-SQL-Port befindet, geben Sie in der Spezifikation der Serverinstanz die Portnummer an. Die Microsoft SQL-Standardportnummer lautet 1433.</p> <p>Beim Aktualisieren der Managerknoten wird die MSSQL-SSL-Option standardmäßig ausgewählt. Wenn Ihre Datenbank SSL nicht verwendet, deaktivieren Sie SSL für Datenbankverbindung verwenden.</p>

- 10 Klicken Sie auf **Weiter**.
- 11 Vergewissern Sie sich, dass alle zu aktualisierenden Dienste auf der Seite „Bereit für Upgrade“ aufgeführt werden, und klicken Sie auf **Aktualisieren**.

Die Aktualisierungsseite und eine Statusanzeige werden angezeigt. Nachdem der Aktualisierungsprozess abgeschlossen ist, wird die Schaltfläche **Weiter** aktiv.

- 12 Klicken Sie auf **Weiter**.
- 13 Klicken Sie auf **Beenden**.

- 14 Vergewissern Sie sich, dass alle Dienste neu gestartet wurden,
- 15 Wiederholen Sie diese Schritte für jeden IaaS-Server in Ihrer Bereitstellung in der angegebenen Reihenfolge.
- 16 Nachdem alle Komponenten aktualisiert wurden, melden Sie sich bei der Verwaltungskonsole der Appliance an und vergewissern Sie sich, dass jetzt alle Dienste, darunter auch IaaS, registriert sind.

Alle ausgewählten Komponenten werden auf die neue Version aktualisiert.

Nächste Schritte

- [Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator-Control Center.](#)
- Wenn in Ihrer Bereitstellung ein Lastausgleichsdienst verwendet wird, aktualisieren Sie für jeden Lastausgleichsknoten die Verwendung von vRealize Automation-Integritätsprüfungen. Aktivieren Sie den Datenverkehr des Lastausgleichsdiensts für alle nicht verbundenen Knoten. Wenn Ihre alte Bereitstellung eine mit einem Lastausgleichsdienst arbeitende, eingebettete PostgreSQL-Datenbank verwendet hat, deaktivieren Sie alle Knoten im PostgreSQL-Pool, da sie überflüssig sind. Löschen Sie bei Gelegenheit den Pool.

Weitere Informationen finden Sie unter [vRealize Automation-Lastausgleich](#).

- (Optional) Aktivieren Sie das automatische Manager Service-Failover. Siehe [Aktivieren des automatischen Manager Service-Failovers nach einem Upgrade](#).

Wiederherstellen des Zugriffs auf das integrierte vRealize Orchestrator -Control Center

Nach dem Upgrade der IaaS-Serverkomponenten müssen Sie den Zugriff auf vRealize Orchestrator wiederherstellen.

Wenn Sie ein Upgrade von vRealize Automation 6.2.5 auf 7.4 durchführen, müssen Sie wie folgt vorgehen, damit die neue Funktion „Rollenbasierte Zugriffssteuerung“ funktioniert. Dieses Verfahren ist für eine Hochverfügbarkeitsumgebung vorgesehen.

Voraussetzungen

Erstellen Sie einen Snapshot Ihrer vRealize Automation-Umgebung.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance-Verwaltungskonsole als Root-Benutzer an, indem Sie den vollqualifizierten Domännennamen des Appliance-Hosts, `https://va-hostname.domain.name:5480` verwenden.
- 2 Wählen Sie **vRA-Einstellungen > Datenbank** aus.
- 3 Identifizieren Sie den Master- und die Replikatknoten.
- 4 Öffnen Sie auf jedem Replikatknoten eine SSH-Sitzung, melden Sie sich als Administrator an und führen Sie den folgenden Befehl aus:

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

- 5 Öffnen Sie auf dem Masterknoten eine SSH-Sitzung, melden Sie sich als Administrator an und führen Sie den folgenden Befehl aus:

```
rm /etc/vco/app-server/vco-registration-id
```

- 6 Wechseln Sie auf dem Masterknoten zum Verzeichnis `/etc/vco/app-server/`.

- 7 Öffnen Sie die Datei `sso.properties`.

- 8 Wenn der Eigenschaftsname `com.vmware.o11n.sso.admin.group.name` Leerzeichen oder andere Bash-Zeichen enthält, die als Sonderzeichen in einem Bash-Befehl akzeptiert werden können, wie etwa einen Bindestrich (-) oder ein Dollarzeichen (\$), führen Sie die folgenden Schritte aus.

- a Kopieren Sie die Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name` und geben Sie als Wert `AdminGroup` ein.
- b Fügen Sie am Beginn der ursprünglichen Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name` ein Hash-Zeichen (#) hinzu, um die Zeile auszukommentieren.
- c Speichern und schließen Sie die Datei `sso.properties`.

- 9 Führen Sie den folgenden Befehl aus:

```
vcac-vami vco-service-reconfigure
```

- 10 Wenn Sie Schritt 8 ausgeführt haben, öffnen Sie die Datei `sso.properties` und führen Sie die folgenden Schritte aus.

- a Entfernen Sie das Hash-Zeichen (#) vom Beginn der ursprünglichen Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name`, um die Auskommentierung der Zeile aufzuheben.
- b Entfernen Sie die Kopie der Zeile mit der Eigenschaft `com.vmware.o11n.sso.admin.group.name`.
- c Speichern und schließen Sie die Datei `sso.properties`.

- 11 Führen Sie den folgenden Befehl aus, um den `vco-server`-Dienst neu zu starten:

```
service vco-server restart
```

- 12 Führen Sie den folgenden Befehl aus, um den `vco-configurator`-Dienst neu zu starten:

```
service vco-configurator restart
```

- 13 Klicken Sie in der vRealize Automation-Appliance-Verwaltungskonsole auf **Dienste** und warten Sie, bis alle Dienste auf dem Masterknoten REGISTRIERT sind.

- 14 Wenn alle Dienste registriert sind, fügen Sie die vRealize Automation-Replikatknoten dem vRealize Automation-Cluster hinzu, um die vRealize Orchestrator-Konfiguration zu synchronisieren. Weitere Informationen hierzu finden Sie unter [Neukonfigurieren des integrierten vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit](#).

Nächste Schritte

[Upgrade von vRealize Orchestrator nach dem Upgrade von vRealize Automation.](#)

Upgrade von vRealize Orchestrator nach dem Upgrade von vRealize Automation

Sie müssen Ihre vRealize Orchestrator-Instanz aktualisieren, nachdem Sie ein Upgrade von vRealize Automation 6.2.5 auf 7.4 durchgeführt haben.

In vRealize Orchestrator 7.4 stehen Ihnen nach einem erfolgreichen Upgrade auf vRealize Automation 7.4 zwei Optionen zur Aktualisierung von vRealize Orchestrator zur Verfügung.

- Sie können Ihren vorhandenen externen vRealize Orchestrator-Server auf die eingebettete vRealize Orchestrator-Instanz aktualisieren, die in vRealize Automation 7.4 enthalten ist.
- Sie können ein Upgrade Ihres vorhandenen eigenständigen oder geclusterten vRealize Orchestrator-Servers durchführen, sodass er mit vRealize Automation 7.4 funktioniert.

Migrieren eines externen vRealize Orchestrator -Servers zu vRealize Automation

Sie können Ihren vorhandenen externen vRealize Orchestrator-Server zu einer in vRealize Automation 7.4 eingebetteten vRealize Orchestrator-Instanz migrieren.

Sie können vRealize Orchestrator als externe Serverinstanz bereitstellen und vRealize Automation für die Verwendung mit dieser externen Instanz konfigurieren oder Sie können den vRealize Orchestrator-Server, der in der vRealize Automation-Appliance enthalten ist, konfigurieren und verwenden.

VMware empfiehlt, dass Sie Ihre externe vRealize Orchestrator-Instanz zu dem Orchestrator-Server migrieren, der in vRealize Automation integriert ist. Die Migration von einer externen zu einer eingebetteten Orchestrator-Instanz bietet folgende Vorteile:

- Reduzierung der Gesamtbetriebskosten
- Vereinfachung des Bereitstellungsmodells
- Verbesserung der betrieblichen Effizienz

Hinweis Ziehen Sie in Betracht, die externe vRealize Orchestrator-Instanz in den folgenden Fällen zu verwenden:

- Mehrere Mandanten in der vRealize Automation-Umgebung
- Geografisch verteilte Umgebung
- Bewältigung von Workloads
- Verwendung bestimmter Plugins, wie z. B. ältere Versionen des Site Recovery Manager-Plugins

Control Center-Unterschiede zwischen externer und eingebetteter Orchestrator-Instanz

Einige Menüoptionen, die im Control Center einer externen vRealize Orchestrator-Instanz verfügbar sind, sind nicht in der Standardansicht des Control Center einer eingebetteten Orchestrator-Instanz enthalten.

Einige Optionen sind im Control Center des eingebetteten Orchestrator-Servers standardmäßig ausgeblendet.

Menüoption	Details
Lizenzierung	Die eingebettete Orchestrator-Instanz ist so vorkonfiguriert, dass vRealize Automation als Lizenzgeber verwendet wird.
Konfiguration exportieren/ importieren	Die Konfiguration der eingebetteten Orchestrator-Instanz ist in den exportierten vRealize Automation-Komponenten enthalten.
Datenbank konfigurieren	Die eingebettete Orchestrator-Instanz verwendet die Datenbank, die von vRealize Automation genutzt wird.
Programm zur Verbesserung der Kundenzufriedenheit	Über die Schnittstelle zur Verwaltung der vRealize Automation-Appliance können Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen. Lesen Sie die Informationen unter <i>Programm zur Verbesserung der Benutzerfreundlichkeit</i> im Handbuch <i>Verwalten von vRealize Automation</i> .

Andere nicht in der Standardansicht des Control Centers sichtbare Optionen sind das Textfeld **Hostadresse** und die Schaltfläche **REGISTRIERUNG AUFHEBEN** auf der Seite **Anbieter für Authentifizierung konfigurieren**.

Hinweis Wenn Sie sich über die vollständige Gruppe der Control Center-Optionen in vRealize Orchestrator, die in vRealize Automation integriert ist, informieren möchten, müssen Sie unter https://vra-va-Hostname.Domäne.Name_oder_Lastausgleichsadresse:8283/vco-controlcenter/#/?advanced die Seite für die erweiterte Verwaltung von Orchestrator aufrufen und diese mit der Funktionstaste F5 auf der Tastatur aktualisieren.

Migrieren einer externen vRealize Orchestrator -Instanz unter Windows zu vRealize Automation

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.4 können Sie Ihre vorhandene externe Instanz von Orchestrator 6.x, die unter Windows installiert ist, zu dem Orchestrator-Server migrieren, der in vRealize Automation 7.4 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Erfolgreiche Migration auf vRealize Automation 7.4.
- Beenden Sie den Orchestrator-Serverdienst auf dem externen Orchestrator-Server.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Laden Sie das Migrationstool vom Orchestrator-Zielserver herunter.
 - a Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
 - b Laden Sie das Archiv `migration-tool.zip` herunter, das sich im Verzeichnis `/var/lib/vco/downloads` befindet.
- 2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.
 - a Legen Sie die Umgebungsvariable `PATH` fest, wobei Sie den `bin`-Ordner der mit Orchestrator installierten Java-JRE wählen.
 - b Laden Sie das Migrationstool auf dem Windows-Server hoch, auf dem der externe Orchestrator-Server installiert ist.
 - c Extrahieren Sie das heruntergeladene Archiv im Orchestrator-Installationsordner.

Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows `C:\Programme\VMware\Orchestrator`.
 - d Führen Sie die Windows-Befehlszeile als Administrator aus und navigieren Sie zum Ordner `bin` im Installationsordner von Orchestrator.

Standardmäßig ist der Pfad zum Ordner `bin` `C:\Programme\VMware\Orchestrator\migration-cli\bin`.
 - e Führen Sie den Befehl `export` über die Befehlszeile aus.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von vRealize Orchestrator zu einem Exportarchiv zusammen.

Das Archiv wird im selben Ordner wie der Ordner `migration-cli` erstellt.

3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.4 integriert ist.

- a Laden Sie die exportierte Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation-Appliance hoch.
- b Ändern Sie im Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` die Zuständigkeit der exportierten Orchestrator-Konfigurationsdatei.

```
chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
```

- c Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
```

4 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE if using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbankname
```

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

5 Wenn Sie vRealize Automation nicht aktualisiert, sondern migriert haben, löschen Sie die vertrauenswürdigen Single Sign-On-Zertifikate aus der Datenbank der eingebettete Orchestrator-Instanz.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

Damit haben Sie erfolgreich eine unter Windows installierte externe vRealize Orchestrator 6.x-Instanz zu einer vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.4 eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance auf vRealize Automation 7.4

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.4 können Sie Ihre vorhandene externe virtuelle Orchestrator 6.x-Appliance auf den Orchestrator-Server migrieren, der in vRealize Automation 7.4 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation-Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Erfolgreiche Migration auf vRealize Automation 7.4.
- Beenden Sie den Orchestrator-Serverdienst auf dem externen Orchestrator-Server.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Laden Sie das Migrationstool vom Orchestrator-Zielservers auf den Orchestrator-Quellserver.
 - a Melden Sie sich bei der virtuellen Appliance vRealize Orchestrator 6.x über SSH als **root** an.
 - b Führen Sie im Verzeichnis `/var/lib/vco` den Befehl `scp` aus, um das Archiv `migration-tool.zip` herunterzuladen.

```
scp root@vra-va-Hostname.Domäne.Name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Führen Sie den Befehl `unzip` zum Extrahieren des Archivs mit den Migrationstools aus.

```
unzip migration-tool.zip
```

2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.

- a Führen Sie im Verzeichnis `/var/lib/vco/migration-cli/bin` den Befehl `export` aus.

```
./vro-migrate.sh export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

Im Ordner `/var/lib/vco` wird ein Archiv mit dem Dateinamen `orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip` erstellt.

3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.4 integriert ist.

- a Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
- b Führen Sie im Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` den Befehl `scp` aus, um das exportierte Konfigurationsarchiv herunterzuladen.

```
scp root@Orchestrator-IP_oder_DNS-Name:/var/lib/vco/orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip ./
```

- c Ändern Sie den Besitzer der exportierten Orchestrator-Konfigurationsdatei.

```
chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
```

- d Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

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

- e Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
```

4 Wenn der externe Orchestrator-Server, von dem aus Sie migrieren möchten, die integrierte PostgreSQL-Datenbank verwendet, bearbeiten Sie deren Datenbankkonfigurationsdateien.

- a Heben Sie in der Datei `/var/vmware/vpostgres/current/pgdata/postgresql.conf` die Kommentierung der Zeile `listen_addresses` auf.
- b Legen Sie als Werte für `listen_addresses` Platzhalter (*) fest.

```
listen_addresses = '*'
```

- c Fügen Sie in der Datei `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` eine Zeile an.

```
host all all vra-va-ip-address/32 md5
```

Hinweis Die Datei `pg_hba.conf` erfordert die Verwendung eines CIDR-Präfixformats anstelle einer IP-Adresse und Subnetzmaske.

- d Starten Sie den PostgreSQL-Serverdienst neu.

```
service vpostgres restart
```

- 5 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

PostgreSQL: `jdbc:postgresql://Host:Port/Datenbankname`

MSSQL: `jdbc:jtds:sqlserver://Host:Port/Datenbankname\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@Host:Port:Datenbankname`

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

- 6 Wenn Sie vRealize Automation nicht aktualisiert, sondern migriert haben, löschen Sie die vertrauenswürdigen Single Sign-On-Zertifikate aus der Datenbank der eingebettete Orchestrator-Instanz.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

- 7 Setzen Sie das System auf die Standardkonfiguration der Datei `postgresql.conf` und `pg_hba.conf` zurück.

- a Starten Sie den PostgreSQL-Serverdienst neu.

Damit haben Sie erfolgreich eine externe virtuelle vRealize Orchestrator 6.x-Appliance auf eine vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.4 eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Konfigurieren des integrierten vRealize Orchestrator -Servers

Nachdem Sie die Konfiguration eines externen Orchestrator-Servers exportiert und in vRealize Automation 7.4 importiert haben, müssen Sie den Orchestrator-Server konfigurieren, der in vRealize Automation integriert ist.

Voraussetzungen

Migrieren Sie die Konfiguration vom externen auf den internen vRealize Orchestrator-Server.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
- 2 Starten Sie den Control Center-Dienst und den Orchestrator-Serverdienst des integrierten vRealize Orchestrator-Servers.

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

- 3 Melden Sie sich beim Control Center des integrierten Orchestrator-Servers als **Administrator** an.

Hinweis Wenn Sie von einer externen vRealize Orchestrator 7.4-Instanz migrieren, fahren Sie mit Schritt 5 fort.

- 4 Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.
- 5 Wenn der externe Orchestrator-Server für den Clustermodus konfiguriert wurde, konfigurieren Sie den Orchestrator-Cluster in vRealize Automation neu.
 - a Rufen Sie die Seite für die erweiterte **Verwaltung des Orchestrator-Clusters** unter `https://vra-va-Hostname.Domäne.Name_oder_Lastausgleichsadresse:8283/vco-controlcenter/#!/control-app/ha?remove-nodes` auf.

Hinweis Wenn die Kontrollkästchen zum **Entfernen** neben den bestehenden Knoten im Cluster nicht angezeigt werden, müssen Sie die Browserseite aktualisieren, indem Sie auf der Tastatur die Funktionstaste F5 drücken.

- b Aktivieren Sie die Kontrollkästchen neben den externen Orchestrator-Knoten und klicken Sie auf **Entfernen**, um sie aus dem Cluster zu entfernen.

- c Wenn Sie die Seite für die erweiterte Verwaltung des Clusters verlassen möchten, löschen Sie die Zeichenfolge `remove-nodes` in der URL und aktualisieren Sie die Browserseite mit der Funktionstaste F5 auf der Tastatur.
 - d Prüfen Sie auf der Seite **Konfiguration überprüfen** im Control Center, ob Orchestrator ordnungsgemäß konfiguriert ist.
- 6 (Optional) Generieren Sie in der Registerkarte **Paketsignaturzertifikat** auf der Seite **Zertifikate** ein neues Paketsignaturzertifikat.
 - 7 (Optional) Ändern Sie die Werte für **Standardmandant** und **Admin-Gruppe** auf der Seite **Anbieter für Authentifizierung konfigurieren**.
 - 8 Stellen Sie sicher, dass der Dienst `vco-server` in der Registerkarte **Dienste** in der Managementkonsole der vRealize Automation-Appliance als REGISTRIERT angezeigt wird.
 - 9 Wählen Sie die `vco`-Dienste des externen Orchestrator-Servers aus und klicken Sie auf **Registrierung aufheben**.

Nächste Schritte

- Importieren Sie alle vertrauenswürdigen Zertifikate aus dem externen Orchestrator-Server in den Trust Store des integrierten Orchestrator-Servers.
- Fügen Sie die vRealize Automation-Replikatknoten zum vRealize Automation-Cluster hinzu, um die Orchestrator-Konfiguration zu synchronisieren.

Weitere Informationen finden Sie in der Beschreibung der *Neukonfiguration der eingebetteten Zielinstanz von vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit* in *Installieren oder Upgrade von vRealize Automation*.

Hinweis Die vRealize Orchestrator-Instanzen werden automatisch zu Clustern zusammengefasst und stehen für die Verwendung zur Verfügung.

- Starten Sie den `vco-configurator`-Dienst auf allen Knoten im Cluster neu.
- Aktualisieren Sie den vRealize Orchestrator-Endpoint, um auf den migrierten integrierten Orchestrator-Server zu verweisen.
- Fügen Sie den vRealize Automation-Host und den IaaS-Host zur Bestandsliste des vRealize Automation-Plug-Ins hinzu, indem Sie die Workflows „Einen vRA-Host hinzufügen“ und „Den IaaS-Host eines vRA-Hosts hinzufügen“ ausführen.

Upgrade einer eigenständigen vRealize Orchestrator Appliance für die Verwendung mit vRealize Automation

Wenn Sie eine eigenständige vRealize Orchestrator Appliance für die Verwendung mit vRealize Automation verwalten, müssen Sie die eigenständige Appliance bei einem Upgrade von vRealize Automation 6.2.5 auf 7.4 aktualisieren.

Eingebettete Instanzen von vRealize Orchestrator werden als Teil der Aktualisierung der vRealize Automation-Appliance aktualisiert. Für eine eingebettete Instanz sind keine zusätzlichen Schritte erforderlich.

Informationen zum Aktualisieren eines vRealize Orchestrator-Appliance-Clusters finden Sie unter [Upgrade eines externen vRealize Orchestrator Appliance-Clusters für die Verwendung mit vRealize Automation](#).

Voraussetzungen

- [Installieren des Updates auf der vRealize Automation-Appliance](#).
- Aktualisieren Sie IaaS-Komponenten wie in [Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation](#) beschrieben.
- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Erhöhen Sie den Arbeitsspeicher der vSphere Orchestrator-Appliance auf mindestens 6 GB. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Erstellen Sie einen Snapshot der virtuellen vSphere Orchestrator-Maschine. Weitere Informationen finden Sie unter *Verwaltung virtueller vSphere-Maschinen* in der vSphere-Dokumentation.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in vSphere Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** im vSphere Control Center.

Verfahren

- 1 Verwenden Sie eines der dokumentierten Verfahren, um Ihre eigenständige Instanz von vRealize Orchestrator zu aktualisieren.
 - [Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys](#).
 - [Aktualisieren von Orchestrator Appliance mithilfe eines ISO-Images](#).
 - [Upgrade von Orchestrator Appliance mithilfe eines angegebenen Repositorys](#).
- 2 Führen Sie im Control Center ein Upgrade des vRealize Automation-NSX-Plug-Ins durch.

Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys

Sie können Orchestrator zum Herunterladen des Upgrade-Pakets aus dem VMware-Standard-Repository konfigurieren.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.

- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter `https://Orchestrator-Server:5480` auf und melden Sie sich als **root** an.
- 2 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
Das Optionsfeld neben der Option **Standard-Repository verwenden** ist aktiviert.
- 3 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.
- 4 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.
- 5 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 6 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 7 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 8 Melden Sie sich beim Control Center als **root** an.
- 9 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

10 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Aktualisieren von Orchestrator Appliance mithilfe eines ISO-Images

Sie können Orchestrator zum Herunterladen eines Upgrade-Pakets aus einer ISO-Imagedatei konfigurieren, die sich auf dem CD-ROM-Laufwerk der Appliance befindet.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.
- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Laden Sie das Archiv `VMware-vRO-Appliance-Version-Build-Nummer-updaterepo.iso` von der offiziellen VMware-Downloadseite herunter.
- 2 Verbinden Sie das CD-ROM-Laufwerk der virtuellen Orchestrator Appliance-Maschine. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- 3 Stellen Sie die ISO-Imagedatei im CD-ROM-Laufwerk der Appliance bereit. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- 4 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter `https://Orchestrator-Server:5480` auf und melden Sie sich als **root** an.
- 5 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
- 6 Aktivieren Sie das Optionsfeld neben der Option **CD-ROM-Updates verwenden**.
- 7 Kehren Sie zur Seite **Status** zurück.
Die Version des verfügbaren Upgrades wird angezeigt.
- 8 Klicken Sie auf **Updates installieren**.
- 9 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 10 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 11 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 12 Melden Sie sich beim Control Center als **root** an.
- 13 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

14 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Upgrade von Orchestrator Appliance mithilfe eines angegebenen Repositorys

Sie können Orchestrator für die Verwendung eines lokalen Repositorys konfigurieren, in das Sie das Upgrade-Archiv hochgeladen haben.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Erhöhen Sie die Festplattengröße der virtuellen vRealize Orchestrator-Maschine: Festplatte1=7 GB, Festplatte2=10 GB.
- Stellen Sie sicher, dass die Root-Partition der Orchestrator Appliance mindestens 3 GB freien Speicherplatz verfügbar hat. Weitere Informationen zum Erhöhen der Größe einer Festplattenpartition finden Sie im KB-Artikel 1004071: <http://kb.vmware.com/kb/1004071>.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Verfahren

- 1 Bereiten Sie das lokale Repository für Upgrades vor.
 - a Installieren und konfigurieren Sie einen lokalen Webserver.
 - b Laden Sie das Archiv `VMware-vRO-Appliance-Version-Build-Nummer-updaterepo.zip` von der offiziellen VMware-Downloadseite herunter.
 - c Extrahieren Sie das ZIP-Archiv in das lokale Repository.
- 2 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter `https://Orchestrator-Server:5480` auf und melden Sie sich als **root** an.
- 3 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.
- 4 Aktivieren Sie das Optionsfeld neben der Option **Angegebenes Repository verwenden**.
- 5 Geben Sie die URL-Adresse des lokalen Repositories an, indem Sie das Verzeichnis `Update_Repo` angeben.
`http://Lokaler_Webserver:Port/build/mts/release/bora-Build-Nummer/publish/exports/Update_Repo`
- 6 Wenn für das lokale Repository eine Authentifizierung erforderlich ist, geben Sie den Benutzernamen und das Kennwort ein.
- 7 Klicken Sie auf **Einstellungen speichern**.
- 8 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.
- 9 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.
- 10 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.
- 11 Starten Sie die Orchestrator Appliance neu, um die Aktualisierung abzuschließen.
 - a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.
- 12 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.
- 13 Melden Sie sich beim Control Center als **root** an.
- 14 Wenn Sie beabsichtigen, einen Cluster von Orchestrator-Instanzen erstellen, konfigurieren Sie die Einstellungen für die Hosts neu.
 - a Klicken Sie auf der Seite **Hosteinstellungen** im Control Center auf **ÄNDERN**.
 - b Geben Sie den Hostnamen des Lastausgleichsservers anstelle des Namens der vRealize Orchestrator Appliance ein.

15 Konfigurieren Sie die Authentifizierung neu.

- a Wenn der Orchestrator-Server vor dem Upgrade dafür konfiguriert wurde, **LDAP** oder **SSO (Legacy)** als Authentifizierungsmethode zu verwenden, konfigurieren Sie **vSphere** oder **vRealize Automation** als Authentifizierungsanbieter.
- b Wenn die Authentifizierung bereits auf **vSphere** oder **vRealize Automation** eingestellt ist, heben Sie die Registrierung der Einstellungen auf und registrieren Sie sie erneut.

Hinweis Wenn Ihr Orchestrator vor dem Upgrade **vSphere** als Authentifizierungsanbieter verwendet hat und so konfiguriert war, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse des vCenter Servers herstellte, müssen Sie, sofern Sie einen externen Platform Services Controller haben, nach dem Upgrade Orchestrator so konfigurieren, dass er eine Verbindung zum vollqualifizierten Domännennamen oder zur IP-Adresse der Platform Services Controller-Instanz, die vCenter Single Sign-On enthält, herstellt. Sie müssen auch die Zertifikate aller Platform Services Controller mit derselben vCenter Single Sign-On-Domäne manuell in Orchestrator importieren.

Damit haben Sie die Orchestrator Appliance erfolgreich aktualisiert.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Upgrade eines externen vRealize Orchestrator Appliance-Clusters für die Verwendung mit vRealize Automation

Wenn Sie einen vRealize Orchestrator Appliance-Cluster mit vRealize Automation verwenden, müssen Sie ein Upgrade des Orchestrator-Appliance-Clusters auf Version 7.4 durchführen, indem Sie eine einzelne Instanz aktualisieren und neu installierte 7.4-Knoten mit der aktualisierten Instanz verbinden.

Voraussetzungen

- [Installieren des Updates auf der vRealize Automation-Appliance.](#)
- Für Sie ein Upgrade der IaaS-Komponenten durch. Siehe [Aktualisieren der IaaS-Serverkomponenten nach dem Upgrade von vRealize Automation.](#)
- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Weitere Informationen finden Sie im [Konfigurationshandbuch für den Lastausgleich von vRealize Orchestrator.](#)
- Erstellen Sie einen Snapshot aller vRealize Orchestrator-Serverknoten.
- Sichern Sie die gemeinsame vRealize Orchestrator-Datenbank.

Verfahren

- 1 Führen Sie im Control Center ein Upgrade des vRealize Automation-NSX-Plug-Ins durch.
- 2 Stoppen Sie auf allen Clusterknoten die Orchestrator-Dienste `vco-server` und `vco-configurator`.

- 3 Aktualisieren Sie nur eine Orchestrator-Serverinstanz in Ihrem Cluster mithilfe eines der dokumentierten Verfahren.
- 4 Stellen Sie eine neue Orchestrator Appliance in Version 7.4 bereit.
 - a Konfigurieren Sie den neuen Knoten mit den Netzwerkeinstellungen einer bereits vorhandenen Instanz, die Teil des Clusters ist, aber noch nicht aktualisiert wurde.
- 5 Rufen Sie das Control Center des zweiten Knotens auf, um den Konfigurationsassistenten zu starten.
 - a Navigieren Sie zu `https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.
- 6 Wählen Sie den Bereitstellungstyp **Orchestrator-Cluster** aus.

Durch die Auswahl dieses Typs wählen Sie aus, dass der Knoten einem vorhandenen Orchestrator-Cluster hinzugefügt werden soll.
- 7 Geben Sie in das Textfeld **Hostname** den Hostnamen oder die IP-Adresse der ersten Orchestrator-Serverinstanz ein.

Hinweis Hierbei muss es sich um die lokale IP-Adresse oder den Hostnamen der Orchestrator-Instanz handeln, der Sie den zweiten Knoten hinzufügen möchten. Verwenden Sie keine Lastausgleichsadresse.

- 8 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des Root-Benutzers für die erste Orchestrator-Serverinstanz ein.
- 9 Klicken Sie auf **Beitreten**. Die Orchestrator-Instanz kloniert die Konfiguration des Knotens, mit dem sie verbunden wird.

Der Orchestrator-Serverdienst beider Knoten wird automatisch neu gestartet.
- 10 Rufen Sie das Control Center des aktualisierten Orchestrator-Clusters über die Lastausgleichsadresse auf, und melden Sie sich als **Administrator** an.
- 11 Stellen Sie auf der Seite **Orchestrator-Clusterverwaltung** sicher, dass die Zeichenfolgen **Aktiver Konfigurationsfingerabdruck** und **Ausstehender Konfigurationsfingerabdruck** auf allen Knoten im Cluster übereinstimmen.

Hinweis Sie müssen die Seite möglicherweise mehrmals aktualisieren, bis die beiden Zeichenfolgen übereinstimmen.

- 12 Vergewissern Sie sich, dass der vRealize Orchestrator-Cluster ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** im Control Center öffnen.
- 13 (Optional) Wiederholen Sie die Schritte 3 bis 8 für jeden weiteren Knoten im Cluster.
- 14 Führen Sie im Control Center ein Upgrade des vRealize Automation-NSX-Plug-Ins durch.

Damit haben Sie den Orchestrator-Cluster aktualisiert.

Nächste Schritte

[Aktivieren der Lastausgleichsdienste.](#)

Hinzufügen von Benutzern oder Gruppen zu einer Active Directory-Verbindung

Sie können Benutzer oder Gruppen zu einer vorhandenen Active Directory-Verbindung hinzufügen.

Das Benutzerauthentifizierungssystem der Verzeichnisverwaltung importiert beim Hinzufügen von Gruppen und Benutzern Daten aus Active Directory. Die Geschwindigkeit des Imports wird durch die Active Directory-spezifischen Datenübertragungsmöglichkeiten beschränkt. Dies führt dazu, dass Aktionen je nach Anzahl der Gruppen und Benutzer, die hinzugefügt werden, viel Zeit in Anspruch nehmen können. Um Probleme zu minimieren, begrenzen Sie die Gruppen und Benutzer auf diejenigen, die für eine vRealize Automation-Aktion erforderlich sind. Falls Probleme auftreten, schließen Sie nicht benötigte Anwendungen und vergewissern Sie sich, dass Active Directory ausreichend Arbeitsspeicher von Ihrer Bereitstellung zugeteilt wurde. Sollten weiterhin Probleme auftreten, erhöhen Sie die Active Directory zugeteilte Menge an Arbeitsspeicher. Bei Bereitstellungen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für Active Directory auf bis zu 24 GB erhöht werden.

Wenn Sie eine vRealize Automation-Bereitstellung mit vielen Benutzern und Gruppen synchronisieren, kann eine Verzögerung eintreten, bevor die Protokolldetails verfügbar sind. Der Zeitstempel der Protokolldatei kann von dem auf der Konsole angezeigten Zeitpunkt der Fertigstellung abweichen.

Wenn Sie eine Gruppe aus Active Directory hinzufügen und Mitglieder der Gruppe nicht in der Benutzerliste enthalten sind, werden diese Mitglieder zur Liste hinzugefügt. Wenn Sie eine Gruppe synchronisieren, werden Benutzer, für die „Domänenbenutzer“ nicht die primäre Gruppe in Active Directory darstellt, nicht synchronisiert.

Hinweis Sie können eine Synchronisierungsaktion nicht abbrechen, nachdem Sie sie gestartet haben.

Voraussetzungen

- Installierter Connector mit aktiviertem Aktivierungscode. Auf der Seite „Benutzerattribute“ können Sie die erforderlichen Standardattribute auswählen und zusätzliche Attribute hinzufügen.

Siehe [PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html](https://plUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html).
- Liste der Active Directory-Gruppen und -Benutzer, die aus Active Directory synchronisiert werden sollen.
- Für Active Directory über LDAP gehören zu den erforderlichen Informationen der Basis-DN, der Bind-DN und das Bind-DN-Kennwort.
- Für die integrierte Windows-Authentifizierung von Active Directory werden die Bind-Benutzer-UPN-Adresse und das entsprechende Kennwort benötigt.
- Wenn auf Active Directory über SSL zugegriffen wird, ist eine Kopie des SSL-Zertifikats erforderlich.

- Wenn Sie Active Directory mit mehreren Gesamtstrukturen und integrierter Windows-Authentifizierung nutzen und die lokale Gruppe der Domäne Mitglieder aus verschiedenen Gesamtstrukturen umfasst, führen Sie die folgenden Schritte aus. Fügen Sie den Bind-Benutzer zur Gruppe „Administratoren“ der lokalen Gruppe der Domäne hinzu. Ohne Hinzufügen des Bind-Benutzers fehlen diese Mitglieder in der lokalen Gruppe der Domäne.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf den gewünschten Verzeichnisnamen.
- 3 Klicken Sie auf **Synchronisierungseinstellungen**, um ein Dialogfeld mit Synchronisierungsoptionen zu öffnen.
- 4 Klicken Sie je nachdem, ob Sie die Benutzerkonfiguration oder die Gruppenkonfiguration ändern möchten, auf das entsprechende Symbol.

So bearbeiten Sie die Gruppenkonfiguration:

- Zum Hinzufügen von Gruppen klicken Sie auf das Symbol **+**, um eine Zeile für Gruppen-DN-Definitionen hinzuzufügen, und geben Sie den entsprechenden Gruppen-DN ein.
- Um eine Gruppen-DN-Definition zu löschen, klicken Sie beim gewünschten Gruppen-DN auf das Symbol **x**.

So bearbeiten Sie die Benutzerkonfiguration:

- ◆ Zum Hinzufügen von Benutzern klicken Sie auf das Symbol **+**, um eine Zeile für eine Benutzer-DN-Definition hinzuzufügen, und geben Sie den entsprechenden Benutzer-DN ein.

Um eine Benutzer-DN-Definition zu löschen, klicken Sie beim gewünschten Benutzer-DN auf das Symbol **x**.

- 5 Klicken Sie auf **Speichern**, um die Änderungen zu speichern, ohne die Aktualisierungen sofort zu synchronisieren. Klicken Sie auf **Speichern und synchronisieren**, um die Änderungen zu speichern und die Aktualisierungen sofort zu synchronisieren.

Aktivieren der Lastausgleichsdienste

Wenn Ihre Bereitstellung Lastausgleichsdienste verwendet, aktivieren Sie die sekundäre Knoten und Integritätsprüfungen erneut und stellen die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst wieder her.

Die Systemzustandsprüfungen für vRealize Automation variieren je nach Version. Informationen finden Sie im *vRealize Automation Load Balancing Configuration Guide* in der [VMware vRealize Automation-Dokumentation](#).

Setzen Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst von 10 Minuten zurück auf den Standardwert.

Aufgaben nach dem Upgrade von vRealize Automation

Nach dem Upgrade von vRealize Automation 6.2.5 auf 7.4 führen Sie alle erforderlichen Aufgaben durch.

Portkonfiguration für Hochverfügbarkeitsbereitstellungen

Nach einem Upgrade in einer Hochverfügbarkeitsbereitstellung müssen Sie den Lastausgleichsdienst so konfigurieren, dass der Datenverkehr an Port 8444 an die vRealize Automation-Appliance geleitet wird, um Remote-Konsolenfunktionen zu unterstützen.

Weitere Informationen finden Sie im *vRealize Automation Load Balancing Configuration Guide* in der [vRealize Automation-Dokumentation](#).

Neukonfigurieren des integrierten vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit

Für eine Hochverfügbarkeitsbereitstellung müssen Sie jede zweiseitige Replikat-Appliance von vRealize Automation mit dem Cluster verbinden, damit die Hochverfügbarkeit für den eingebetteten vRealize Orchestrator unterstützt wird.

Voraussetzungen

Melden Sie sich bei der zweiseitigen Verwaltungskonsole der vRealize Automation-Replikat-Appliance an.

- 1 Starten Sie einen Browser und öffnen Sie die Verwaltungskonsole der zweiseitigen Replikat-vRealize Automation-Appliance mithilfe des vollqualifizierten Domänennamens (FQDN) der zweiseitigen virtuellen Replikat-Appliance: `https://vra-va-hostname.domain.name:5480`.
- 2 Melden Sie sich mit dem beim Bereitstellen der zweiseitigen Replikat-vRealize Automation-Appliance eingegebenen Benutzernamen **Root** und dem zugehörigen Kennwort an.

Verfahren

- 1 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 2 Geben Sie in das Textfeld **Führender Clusterknoten** den FQDN der zweiseitigen vRealize Automation-Master-Appliance an.
- 3 Geben Sie das Root-Kennwort in das Textfeld **Kennwort** ein.
- 4 Klicken Sie auf **Cluster beitreten**.
Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort. Das System startet die Dienste für den Cluster neu.
- 5 Stellen Sie sicher, dass alle Dienste ausgeführt werden.
 - a Klicken Sie auf der obersten Registerkartenleiste auf **Dienste**.
 - b Klicken Sie auf **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Aktivieren der Aktion „Mit Remote-Konsole verbinden“ für Verbraucher

Die Remote-Konsolen-Aktion für Verbraucher wird für Appliances unterstützt, die von vSphere in vRealize Automation bereitgestellt werden.

Bearbeiten Sie den Blueprint, nachdem Sie ein Versions-Upgrade ausgeführt haben, und wählen Sie die Aktion **Mit Remote-Konsole verbinden** auf der Registerkarte **Aktion** aus.

Weitere Informationen finden Sie im [Knowledgebase-Artikel 2109706](#).

Wiederherstellen von Dateien für die Zeitüberschreitung bei externen Workflows

Sie müssen die Dateien für die Zeitüberschreitung bei externen Workflows in vRealize Automation neu konfigurieren, da der Upgradevorgang die XMLDB-Dateien überschreibt.

Verfahren

- 1 Öffnen Sie die Konfigurationsdateien für den externen Workflow (xmlldb) auf dem System über das folgende Verzeichnis.

```
\\VMware\vcac\Server\ExternalWorkflows\xmlldb\.
```

- 2 Ersetzen Sie die XMLDB-Dateien durch die Dateien, die Sie vor der Migration gesichert haben. Wenn Sie über keine Sicherungsdateien verfügen, konfigurieren Sie die Einstellungen für die Zeitüberschreitung bei externen Workflows.
- 3 Speichern Sie Ihre Einstellungen.

Überprüfen, ob der vRealize Orchestrator -Dienst verfügbar ist

Nach dem Upgrade auf die neueste Version von vRealize Automation müssen Sie die Verbindung zwischen vRealize Automation und vRealize Orchestrator überprüfen. Manchmal müssen Sie nach einem Upgrade die Verbindung wiederherstellen.

Voraussetzungen

Melden Sie sich bei der Konfigurationsschnittstelle von vRealize Orchestrator an.

Verfahren

- 1 Klicken Sie auf **Konfiguration validieren**.
- 2 Wenn der Abschnitt „Authentifizierung“ mit einem grünen Häkchen versehen ist, fahren Sie mit Schritt 5 fort.
- 3 Wenn der Abschnitt „Authentifizierung“ nicht mit einem grünen Häkchen versehen ist, führen Sie die folgenden Schritte aus, um die Verbindung zu vRealize Orchestrator wiederherzustellen.
 - a Klicken Sie auf **Home**.
 - b Klicken Sie auf **Authentifizierungsanbieter konfigurieren**.
 - c Wählen Sie im Textfeld **Admin-Gruppe** die Option **Ändern** aus und wählen Sie eine neue Admin-Gruppe aus, die ordnungsgemäß aufgelöst werden kann.

Die Gruppe „vcoadmins“ ist nur im standardmäßigen Mandanten „vsphere.local“ verfügbar. Wenn Sie einen anderen Mandanten für vRealize Orchestrator verwenden, müssen Sie eine andere Gruppe auswählen.

- d Klicken Sie auf **Änderungen speichern** und starten Sie den vRealize Orchestrator-Server bei Aufforderung neu.
 - e Klicken Sie auf **Home**.
- 4 Wiederholen Sie Schritt 1, um zu überprüfen, ob der Abschnitt „Authentifizierung“ immer noch mit einem grünen Häkchen versehen ist.
 - 5 Klicken Sie auf **Home** und schließen Sie das vRealize Orchestrator Control Center.

Neukonfiguration eingebetteter vRealize Orchestrator -Infrastruktur-Endpoints in der vRealize Automation -Zielumgebung

Bei der Migration von einer vRealize Automation 6.2.x-Umgebung müssen Sie die URL des Infrastruktur-Endpoints aktualisieren, die auf den zieleseitigen eingebetteten vRealize Orchestrator-Server verweist.

Voraussetzungen

- Führen Sie eine erfolgreiche Migration auf vRealize Automation 7.4 durch.
- Melden Sie sich an der zieleseitigen vRealize Automation-Konsole an.
 - a Öffnen Sie die vRealize Automation-Konsole unter Angabe des vollqualifizierten Domännennamens der zieleseitigen virtuellen Appliance: `https://vra-va-hostname.domain.name/vcac`.

Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domännennamens des Lastausgleichsdiensts der zieleseitigen virtuellen Appliance: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Melden Sie sich als IaaS-Administrator an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie auf der Seite „Endpoints“ den vRealize Orchestrator-Endpoint aus und klicken Sie auf **Bearbeiten**.
- 3 Bearbeiten Sie im Textfeld „Adresse“ die vRealize Orchestrator-Endpoint-URL.
 - Wenn Sie eine Migration in eine minimale Umgebung durchgeführt haben, ersetzen Sie die vRealize Orchestrator-Endpoint-URL durch `https://vra-va-hostname.domain.name:443/vco`.
 - Wenn Sie eine Migration in eine Hochverfügbarkeitsumgebung durchgeführt haben, ersetzen Sie die vRealize Orchestrator-Endpoint-URL durch `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Klicken Sie auf **OK**.
- 5 Führen Sie manuell eine Datenerfassung auf dem vRealize Orchestrator-Endpoint aus.
 - a Wählen Sie auf der Seite „Endpoints“ den vRealize Orchestrator-Endpoint aus.
 - b Wählen Sie **Aktionen > Datenerfassung** aus.Stellen Sie sicher, dass die Datenerfassung erfolgreich verläuft.

Wiederherstellung von vorgenommenen Änderungen an der Protokollierung in der `app.config`-Datei

Der Upgrade-Vorgang überschreibt Änderungen, die Sie an der Protokollierung vornehmen, in den Konfigurationsdateien. Nach Abschluss eines Upgrades müssen Sie alle Änderungen wiederherstellen, die Sie vor dem Upgrade an der Datei `app.config` vorgenommen haben.

Aktivieren des automatischen Manager Service-Failovers nach einem Upgrade

Das automatische Manager Service-Failover ist standardmäßig deaktiviert, wenn Sie vRealize Automation aktualisieren.

Führen Sie diese Schritte durch, um das automatische Manager Service-Failover nach einem Upgrade zu aktivieren.

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung als Root-Benutzer auf der vRealize Automation-Appliance.
- 2 Wechseln Sie zum Verzeichnis `/usr/lib/vcac/tools/vami/commands`.
- 3 Um das automatische Manager Service-Failover zu aktivieren, führen Sie den folgenden Befehl aus.

```
python ./manager-service-automatic-failover ENABLE
```

Um das automatische Failover in der gesamten IaaS-Bereitstellung zu deaktivieren, führen Sie den folgenden Befehl aus.

```
python ./manager-service-automatic-failover DISABLE
```

Informationen zum automatischen Manager Service-Failover

Sie können den vRealize Automation IaaS Manager Service so konfigurieren, dass automatisch ein Failover zu einem Backup durchgeführt wird, wenn der primäre Manager Service beendet wird.

Ab vRealize Automation 7.3 müssen Sie den Manager Service nicht mehr auf jedem Windows-Server manuell starten oder beenden, um zu steuern, welcher Server als primärer Server oder als Backup dient. Das automatische Manager Service-Failover ist standardmäßig deaktiviert, wenn Sie das Upgrade von IaaS mit dem Upgrade-Shell-Skript oder mit der ausführbaren Datei für das IaaS-Installationsprogramm durchführen.

Wenn automatisches Failover aktiviert ist, wird der Manager Service automatisch auf allen Manager Service-Hosts, einschließlich der Backups, gestartet. Die automatische Failover-Funktion ermöglicht die gegenseitige transparente Überwachung der Hosts und die Durchführung eines Failovers bei Bedarf. Der Windows-Dienst muss jedoch auf allen Hosts ausgeführt werden.

Hinweis Es ist nicht erforderlich, automatisches Failover zu verwenden. Sie können diese Funktion deaktivieren und den Windows-Dienst weiterhin manuell starten und beenden, um zu steuern, welcher Host als primärer Host oder als Backup dient. Beim manuellen Failover müssen Sie den Dienst nur jeweils auf einem Host starten. Bei deaktiviertem automatischem Failover führt die gleichzeitige Ausführung des Diensts auf mehreren IaaS-Servern dazu, dass vRealize Automation nicht mehr verwendet werden kann.

Versuchen Sie nicht, automatisches Failover selektiv zu aktivieren oder zu deaktivieren. Automatisches Failover muss immer auf jedem Manager Service-Host in einer IaaS-Bereitstellung als aktiviert oder deaktiviert synchronisiert werden.

Ausführen einer Testverbindung und Überprüfen von aktualisierten Endpoints

Beim Upgrade von vRealize Automation 7.3 oder früher auf 7.4 werden Änderungen an Endpoints in der Zielumgebung vorgenommen.

Nach dem Upgrade auf vRealize Automation 7.4 müssen Sie die Aktion **Testverbindung** für alle anwendbaren Endpoints durchführen. Außerdem müssen Sie möglicherweise einige aktualisierte Endpoints anpassen. Weitere Informationen finden Sie unter [Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints](#).

Die Standardsicherheitseinstellung für aktualisierte oder migrierte Endpoints ist, nicht vertrauenswürdige Zertifikate nicht zu akzeptieren.

Wenn Sie nicht vertrauenswürdige Zertifikate verwendet haben, müssen Sie nach dem Upgrade oder der Migration von einer früheren vRealize Automation-Installation die folgenden Schritte für alle vSphere- und NSX-Endpoints ausführen, um die Validierung des Zertifikats durchzuführen. Andernfalls schlagen die Endpoint-Vorgänge mit Zertifikatsfehlern fehl. Weitere Informationen finden Sie in den VMware Knowledgebase-Artikeln *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* unter <http://kb.vmware.com/kb/2150230> und *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* unter <http://kb.vmware.com/kb/2108294>.

- 1 Melden Sie sich nach dem Upgrade bzw. der Migration bei der vRealize Automation vSphere-Agent-Maschine an und starten Sie Ihre vSphere-Agents mithilfe der Registerkarte **Dienste** neu.

Im Fall einer Migration werden möglicherweise nicht alle Agents neu gestartet. Starten Sie diese bei Bedarf manuell neu.

- 2 Warten Sie, bis mindestens ein Ping-Bericht abgeschlossen ist. Es dauert eine oder zwei Minuten, bis ein Ping-Bericht abgeschlossen ist.
- 3 Wenn die vSphere-Agents die Datenerfassung gestartet haben, melden Sie sich bei vRealize Automation als IaaS-Administrator an.
- 4 Klicken Sie auf **Infrastruktur > Endpoints > Endpoints**.
- 5 Bearbeiten Sie einen vSphere-Endpoint und klicken Sie auf **Verbindung testen**.
- 6 Wenn eine Zertifikataufforderung angezeigt wird, klicken Sie auf **OK**, um das Zertifikat zu akzeptieren.

Wenn keine Zertifikataufforderung angezeigt wird, kann es sein, dass das Zertifikat derzeit korrekt in einer vertrauenswürdigen Rootzertifizierungsstelle der Windows-Maschine gespeichert ist, die Dienste für den Endpoint hostet, z. B. als Proxy-Agent-Maschine oder DEM-Maschine.

- 7 Klicken Sie auf **OK**, um die Zertifikatsannahme anzuwenden und den Endpoint zu speichern.
- 8 Wiederholen Sie diesen Vorgang für jeden vSphere-Endpoint.
- 9 Wiederholen Sie diesen Vorgang für jeden NSX-Endpoint.

Wenn die Aktion **Verbindung testen** erfolgreich war, aber einige Datenerfassungs- bzw. Bereitstellungsvorgänge fehlschlagen, können Sie dasselbe Zertifikat auf allen Agent-Maschinen installieren, die den Endpoint bedienen, sowie auf allen DEM-Maschinen. Alternativ dazu können Sie das Zertifikat von vorhandenen Maschinen deinstallieren und den oben genannten Vorgang für den fehlerhaften Endpoint wiederholen.

Importieren des DynamicTypes-Plug-Ins

Wenn Sie das DynamicTypes-Plug-In verwenden und die Konfiguration vor dem Upgrade als Paket exportiert haben, müssen Sie den folgenden Workflow importieren:

```
/Library/Dynamic Types/Configuration/Import Configuration From Package
```

Der /Library-Befehl wird über den Java-Client von vRealize Orchestrator ausgeführt.

Fehlerbehebung bei vRealize Automation -Upgrades

Die Themen zur Fehlerbehebung bei einem Upgrade bieten Lösungen für Probleme, die beim Upgrade von vRealize Automation 6.2.5 auf 7.4 auftreten können.

Installations- oder Aktualisierungsfehler mit einem Zeitüberschreitungsfehler des Lastausgleichsdiensts

Ein(e) vRealize Automation-Installation bzw. -Upgrade für eine verteilte Bereitstellung mit einem Lastausgleichsdienst schlägt mit Fehler 503 „Dienst nicht verfügbar“ fehl.

Problem

Die Installation bzw. das Upgrade schlägt fehl, da der Zeitüberschreitungswert für den Lastausgleichsdienst nicht genügend Zeit zum Abschluss der Aufgabe einräumt.

Ursache

Ein unzureichender Zeitüberschreitungswert für den Lastausgleichsdienst kann zu einem Fehler führen. Sie können das Problem beheben, indem Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden erhöhen und die Aufgabe erneut ausführen.

Lösung

- 1 Erhöhen Sie den Zeitüberschreitungswert für den Lastausgleichsdienst auf mindestens 100 Sekunden.
- 2 Führen Sie die Installation bzw. das Upgrade erneut aus.

Upgrade für die IaaS-Website-Komponente schlägt fehl

Das IaaS-Upgrade schlägt fehl und Sie können das Upgrade nicht fortsetzen.

Problem

Das Iaas-Upgrade schlägt für die Website-Komponente fehl. Die folgenden Fehlermeldungen werden in der Protokolldatei des Installationsprogramms angezeigt.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

Die folgenden Fehlermeldungen werden in der Repository-Protokolldatei angezeigt.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at

```
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core-
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Ursache

Das IaaS-Upgrade schlägt fehl, wenn das Erstellungsdatum für die Datei `web.config` dasselbe oder ein späteres ist als das Datum der Änderung.

Lösung

- 1 Melden Sie sich auf dem IaaS-Host bei Windows an.
- 2 Öffnen Sie die Windows-Eingabeaufforderung.
- 3 Wechseln Sie zum vRealize Automation-Installationsverzeichnis.
- 4 Starten Sie Ihren bevorzugten Text-Editor mit der Option **Als Administrator ausführen**.
- 5 Suchen und wählen Sie die Datei `web.config` aus und speichern Sie die Datei, um das Änderungsdatum zu ändern.
- 6 Überprüfen Sie die Eigenschaften der Datei `web.config`, um zu bestätigen, dass das Änderungsdatum hinter dem Erstellungsdatum liegt.
- 7 Führen Sie ein Upgrade von IaaS aus.

Manager Service kann aufgrund von SSL-Validierungsfehlern während der Laufzeit nicht ausgeführt werden

Der Manager Service kann aufgrund von SSL-Validierungsfehlern nicht ausgeführt werden.

Problem

Der Manager Service kann nicht ausgeführt werden und im Protokoll wird die folgende Fehlermeldung angezeigt:

[Info]: Thread-Id="6" – context="" token="" Fehler beim Verbinden mit der Hauptdatenbank, erneuter Versuch in 00:00:05, Fehlerdetails: Eine Verbindung mit dem Server wurde erfolgreich hergestellt, aber dann ist während des Anmeldevorgangs ein Fehler aufgetreten. (Anbieter: SSL-Anbieter, Fehler: 0 – Die Zertifikatkette wurde von einer Autorität ausgestellt, der nicht vertraut wird.)

Ursache

Während der Laufzeit kann der Manager Service aufgrund von SSL-Validierungsfehlern nicht ausgeführt werden.

Lösung

- 1 Öffnen Sie die Konfigurationsdatei `ManagerService.config`.
- 2 Aktualisieren Sie in der folgenden Zeile die entsprechende Einstellung auf **Encrypt=False**:

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Fehlschlagen der Anmeldung nach dem Upgrade

Nach einem Upgrade müssen Sie für die Sitzungen den Browser beenden und sich neu anmelden, die nicht synchronisierte Benutzerkonten verwenden.

Problem

Nach dem Upgrade von vRealize Automation verweigert das System bei der Anmeldung den Zugriff auf nicht synchronisierte Benutzerkonten.

Lösung

Beenden Sie den Browser und starten Sie vRealize Automation neu.

Katalogelemente werden nach dem Upgrade im Servicekatalog aufgeführt, können aber nicht angefordert werden

Katalogelemente, die bestimmte Eigenschaftsdefinitionen aus früheren Versionen verwenden, werden im Servicekatalog zwar angezeigt, können aber nach dem Upgrade auf die neueste Version von vRealize Automation nicht angefordert werden.

Problem

Wenn Sie ein Upgrade von 6.2.x oder einer früheren Version durchgeführt haben und Eigenschaftsdefinitionen mit den folgenden Steuerungstypen oder Attributen vorhanden waren, fehlen die Attribute in den Eigenschaftsdefinitionen. Katalogelemente, die diese Definitionen verwenden, funktionieren nicht mehr auf dieselbe Weise wie vor der Durchführung des Upgrades.

- Steuerungstypen. Kontrollkästchen oder Verknüpfung.
- Attribute. Beziehung, reguläre Ausdrücke oder Eigenschaftslayouts.

Ursache

In vRealize Automation 7.0 und höher werden in Eigenschaftsdefinitionen keine Attribute mehr verwendet. Sie müssen die Eigenschaftsdefinitionen neu erstellen oder sie neu konfigurieren, sodass eine vRealize Orchestrator-Skriptaktion anstelle der eingebetteten Steuerungstypen oder Attribute verwendet wird.

Migrieren Sie den Steuerungstyp oder die Attribute mithilfe einer Skriptaktion auf vRealize Automation 7.x.

Lösung

- 1 Erstellen Sie in vRealize Orchestrator eine Skriptaktion, die die Eigenschaftswerte zurückgibt. Die Aktion muss einen einfachen Typ zurückgeben, beispielsweise Zeichenfolgen, ganze Zahlen oder andere unterstützte Typen. In der Aktion können andere Eigenschaften, von denen sie abhängt, als Eingabeparameter angegeben werden.
- 2 Konfigurieren Sie die Produktdefinition in der vRealize Automation-Konsole.
 - a Wählen Sie **Administration > Eigenschaftenwörterbuch > Eigenschaftsdefinitionen** aus.
 - b Wählen Sie die Eigenschaftsdefinition aus und klicken Sie auf **Bearbeiten**.
 - c Wählen Sie aus dem Dropdown-Menü „Anzeigehinweis“ die Option **Dropdown** aus.
 - d Wählen Sie aus dem Dropdown-Menü „Werte“ die Option **Externe Werte** aus.
 - e Wählen Sie die Skriptaktion aus.
 - f Klicken Sie auf **OK**.
 - g Konfigurieren Sie die in der Skriptaktion enthaltenen Eingabeparameter. Um die bereits vorhandene Beziehung beizubehalten, binden Sie den Parameter an die andere Eigenschaft.
 - h Klicken Sie auf **OK**.

Zusammenführen externer PostgreSQL-Datenbanken ist nicht erfolgreich

Die Zusammenführung der externen PostgreSQL-Datenbank mit der eingebetteten PostgreSQL-Datenbank war nicht erfolgreich.

Problem

Wenn die externe PostgreSQL-Datenbankversion höher als die eingebettete PostgreSQL-Datenbankversion ist, schlägt die Zusammenführung fehl.

Lösung

- 1 Melden Sie sich beim Host für die externe PostgreSQL-Datenbank an.
- 2 Führen Sie den Befehl `psql --version` aus.
Notieren Sie sich die PostgreSQL-Version für die externe Datenbank.
- 3 Melden Sie sich beim Host für die eingebettete PostgreSQL-Datenbank an.

4 Führen Sie den Befehl `psql --version` aus.

Notieren Sie sich die PostgreSQL-Version für die eingebettete Datenbank.

Wenn die externe PostgreSQL-Version höher als die eingebettete PostgreSQL-Version ist, wenden Sie sich an den Support, um Hilfe bei der Zusammenführung Ihrer externen PostgreSQL-Datenbank zu erhalten.

Befehl „Cluster beitreten“ schlägt scheinbar fehl nach einem Upgrade einer Hochverfügbarkeitsumgebung

Nachdem Sie in der Managementkonsole eines sekundären Cluster-Knotens auf **Cluster beitreten** geklickt haben, wird die Statusanzeige nicht mehr angezeigt.

Problem

Wenn Sie die Verwaltungskonsole der vRealize Automation-Appliance nach dem Upgrade verwenden, um einen sekundären Clusterknoten zum primären Knoten hinzuzufügen, wird die Statusanzeige nicht mehr angezeigt und es wird weder eine Fehlermeldung noch eine Erfolgsmeldung angezeigt. Bei diesem Verhalten handelt es sich um ein zeitweiliges Problem.

Ursache

Die Statusanzeige wird nicht mehr angezeigt, da einige Browser aufhören, auf eine Antwort vom Server zu warten. Der Clusterbeitrittsvorgang wird durch dieses Verhalten nicht beendet. Mithilfe der Protokolldatei unter `/var/log/vmware/vcac/vcac-config.log` können Sie überprüfen, ob der Clusterbeitrittsvorgang erfolgreich war.

Upgrade ist nicht erfolgreich, wenn die Root-Partition nicht über ausreichend freien Speicherplatz verfügt

Wenn nicht genug freier Speicherplatz auf der Root-Partition des Hosts der vRealize Automation-Appliance verfügbar ist, kann das Upgrade nicht fortgesetzt werden.

Lösung

Mit diesem Verfahren wird der freie Speicherplatz auf der Root-Partition der Festplatte 1 des Hosts der vRealize Automation-Appliance erhöht. Führen Sie in einer verteilten Umgebung dieses Verfahren durch, um den freien Speicherplatz auf den Replikatknoten nacheinander zu erhöhen, und erhöhen Sie anschließend den freien Speicherplatz auf dem Master-Knoten.

Hinweis Wenn Sie diesen Vorgang ausführen, werden möglicherweise die folgenden Warnmeldungen angezeigt:

- ```
WARNING: Re-reading the partition table failed with error 16:
Device or resource busy. The kernel still uses the old table. The
new table will be used at the next reboot or after you run
partprobe(8) or kpartx(8) Syncing disks.
```
- ```
Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel
of the change, probably because it/they are in use. As a result, the old partition(s) will remain
in use. You should reboot now before making further changes.
```

Ignorieren Sie die Meldung Sie sollten jetzt einen Neustart durchführen, bevor Sie weitere Änderungen vornehmen. Wenn Sie das System vor Schritt 10 neu starten, wird der Upgrade-Vorgang unterbrochen.

Verfahren

- 1 Schalten Sie die virtuelle Hostmaschine der vRealize Automation-Appliance ein, und melden Sie sich mit einer Secure Shell-Verbindung als Root-Benutzer an.
- 2 Führen Sie die folgenden Befehle aus, um die Dienste zu beenden.
 - a `service vcac-server stop`
 - b `service vco-server stop`
 - c `service vpostgres stop`
- 3 Führen Sie den folgenden Befehl zum Unmounten der Auslagerungspartition durch.

```
swapoff -a
```
- 4 Führen Sie den folgenden Befehl aus, um die vorhandenen Festplatte 1-Partitionen zu löschen und eine 44-GB-Root-Partition sowie eine 6-GB-Auslagerungspartition zu erstellen.

```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G';
echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```
- 5 Führen Sie den folgenden Befehl aus, um den Typ der Auslagerungspartition zu ändern.

```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```
- 6 Führen Sie den folgenden Befehl aus, um das Start-Flag für Festplatte 1 zu setzen.

```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 Führen Sie den folgenden Befehl aus, um die Partitionsänderungen beim Linux-Kernel zu registrieren.

```
partprobe
```

Wenn eine Meldung angezeigt wird, in der Sie zur Durchführung eines Neustarts aufgefordert werden, bevor Sie weitere Änderungen vornehmen, können Sie diese ignorieren. Durch einen Neustart des Systems vor Schritt 10 wird der Upgradevorgang unterbrochen.

- 8 Führen Sie den folgenden Befehl aus, um die neue Auslagerungspartition zu formatieren.

```
mkswap /dev/sda2
```

- 9 Führen Sie den folgenden Befehl aus, um die Auslagerungspartition zu mounten.

```
swapon -a
```

- 10 Neustarten der vRealize Automation-Appliance.

- 11 Führen Sie nach dem Neustart der Appliance den folgenden Befehl aus, um die GröÙer der Partitionstabelle von Festplatte 1 zu ändern.

```
resize2fs /dev/sda1
```

- 12 Um sicherzustellen, dass die Festplattenerweiterung erfolgreich war, führen Sie den Befehl `df -h` aus und prüfen Sie, ob der verfügbare Festplattenspeicher auf `/dev/sda1` größer als 30 GB ist.

Sicherungskopien von XML-Dateien führen zu einer Zeitüberschreitung des Systems

vRealize Automation registriert alle Dateien mit der Erweiterung „.xml“ im Verzeichnis „\VMware\CAC\Server\ExternalWorkflows\xml\“. Wenn dieses Verzeichnis Sicherungsdateien mit der Erweiterung „.xml“ enthält, führt das System doppelte Workflows aus, die zu einer Zeitüberschreitung des Systems führen.

Lösung

Problemumgehung: Wenn Sie Dateien in diesem Verzeichnis sichern, verschieben Sie die Sicherungskopien in ein anderes Verzeichnis oder ändern Sie den Dateierweiterungsamen der Sicherungsdatei in eine andere Erweiterung als „.xml“.

Löschen von verwaisten Knoten in vRealize Automation

Ein verwaister Knoten ist ein doppelter Knoten, der auf dem Host gemeldet wird, aber auf dem Host nicht existiert.

Problem

Wenn Sie überprüfen, ob sich alle IaaS- und virtuellen Appliance-Knoten in fehlerfreiem Zustand befinden, stellen Sie möglicherweise fest, dass es auf einem Host einen oder mehrere verwaiste Knoten gibt. Sie müssen alle verwaisten Knoten löschen.

Lösung

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsole der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
- 2 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 3 Klicken Sie für jeden verwaisten Knoten in der Tabelle auf **Löschen**.

Es kann kein neues Verzeichnis in vRealize Automation erstellt werden

Der Versuch, dem ersten Sync-Konnektor ein neues Verzeichnis hinzuzufügen, schlägt fehl.

Problem

Dieses Problem tritt aufgrund einer fehlerhaften Datei `config-state.json` im Verzeichnis `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/` auf.

Weitere Informationen zum Beheben dieses Problems finden Sie im [Knowledgebase-Artikel 2145438](#).

Für einige virtuelle Maschinen wird während des Upgrades keine Bereitstellung erstellt

Virtuelle Maschinen, die zum Zeitpunkt des Upgrades den Status „Fehlt“ aufweisen, verfügen nicht über eine entsprechende in der Zielumgebung erstellte Bereitstellung.

Problem

Wenn eine virtuelle Maschine in der Quellumgebung während des Upgrades den Status „Fehlt“ aufweist, wird in der Zielumgebung keine entsprechende Bereitstellung erstellt. Wenn eine virtuelle Maschine nach dem Upgrade den Status „Fehlt“ verlässt, können Sie die Maschine unter Verwendung der Massenimportfunktion in die Zielumgebung importieren.

Fehler „Zertifikat nicht vertrauenswürdig“

Wenn Sie die Seite „Protokoll-Viewer“ in der vRealize Automation-Appliance-Konsole öffnen, wird möglicherweise ein Fehlerbericht für eine Endpoint-Verbindung mit diesen Worten angezeigt: `Certificate is not trusted`.

Problem

Wählen Sie auf der vRealize Automation-Appliance-Konsole **Infrastruktur > Überwachung > Protokoll** aus. Auf der Seite „Protokoll-Viewer“ wird möglicherweise ein Bericht ähnlich dem Folgenden angezeigt:

Failed to connect to the endpoint. To validate that a secure connection can be established to this endpoint, go to the vSphere endpoint on the Endpoints page and click the Test Connection button.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.my-company.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Ursache

Das Upgrade von vRealize Automation 7.3 oder früher auf 7.4 nimmt Änderungen an den Endpoints der ursprünglichen Umgebung vor. In Umgebungen, die kürzlich auf vRealize Automation 7.4 aktualisiert wurden, muss der IaaS-Administrator jeden vorhandenen Endpoint überprüfen, der eine sichere HTTPS-Verbindung verwendet. Wenn für einen Endpoint der Fehler `Certificate is not trusted` angezeigt wird, funktioniert der Endpoint nicht ordnungsgemäß.

Lösung

- 1 Melden Sie sich bei der vRealize Automation-Konsole als Infrastrukturadministrator an.
- 2 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 3 Führen Sie diese Schritte für jeden Endpoint mit einer sicheren Verbindung durch.
 - a Klicken Sie auf **Bearbeiten**.
 - b Klicken Sie auf **Testverbindung**.
 - c Überprüfen Sie die Zertifikatdetails und klicken Sie auf **OK**, wenn Sie das Zertifikat als vertrauenswürdig einstufen.
 - d Starten Sie die Windows-Dienste für alle IaaS-Proxy-Agents, die von diesem Endpoint verwendet werden.
- 4 Stellen Sie sicher, dass keine Fehler `Certificate is not trusted` auf der Seite „Protokoll-Viewer“ mehr angezeigt werden.

Installation von oder Upgrade auf vRealize Automation schlägt fehl

Die Installation oder das Upgrade von vRealize Automation schlägt fehl, und in der Protokolldatei wird eine Fehlermeldung angezeigt.

Problem

Wenn Sie vRealize Automation installieren oder ein Upgrade dazu durchführen, schlägt der Vorgang fehl. Dies geschieht in der Regel, wenn ein Fix, der während der Installation oder des Upgrades angewendet wird, nicht erfolgreich ist. In der Protokolldatei wird eine Fehlermeldung ähnlich der folgenden angezeigt: `Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.`

Ursache

Die Windows-Umgebung hat eine Gruppenrichtlinie für die Ausführung von PowerShell-Skripten auf „Aktiviert“ gesetzt.

Lösung

- 1 Führen Sie auf der Windows-Hostmaschine `gpedit.msc` aus, um den lokalen Gruppenrichtlinien-Editor zu öffnen.
- 2 Klicken Sie im linken Bereich unter **Computerkonfiguration** auf die Schaltfläche zum Erweitern, um **Administrative Vorlagen > Windows-Komponenten > Windows PowerShell** zu öffnen.

3 Ändern Sie die Einstellung von **Skriptausführung aktivieren** von Enabled in Not Configured.

Beim Update wird kein Upgrade des Management Agents durchgeführt

Eine Fehlermeldung bezüglich des Verwaltungsagenten wird angezeigt, wenn Sie auf der Seite „Status aktualisieren“ der vRealize Automation-Appliance-Verwaltungskonsole auf **Updates installieren** klicken.

Problem

Upgrade-Prozess ist fehlgeschlagen. Folgende Fehlermeldung wird angezeigt: Management-Agent auf Knoten x konnte nicht aktualisiert werden. In manchen Fällen werden in dieser Meldung mehrere Knoten aufgelistet.

Ursache

Für dieses Problem gibt es zahlreiche Ursachen. In der Fehlermeldung wird nur die Knoten-ID der betroffenen Maschine angegeben. Weitere Informationen finden Sie in der Datei ALL.log für den Management-Agent auf der Maschine, auf der der Befehl fehlgeschlagen ist.

Führen Sie diese Aufgaben entsprechend der bei Ihnen vorliegenden Situation auf den betroffenen Knoten durch:

Lösung

- Wenn der Management-Agent-Dienst nicht ausgeführt wird, starten Sie den Dienst und starten Sie das Upgrade auf der virtuellen Appliance neu.
- Wenn der Management-Agent-Dienst ausgeführt wird und ein Upgrade des Management-Agents durchgeführt wird, starten Sie das Upgrade auf der virtuellen Appliance neu.
- Wenn der Management-Agent-Dienst ausgeführt wird, jedoch kein Upgrade des Management-Agents durchgeführt wird, führen Sie ein manuelles Upgrade durch.
 - a Öffnen Sie einen Browser und wechseln Sie zur Seite „vRealize Automation-aaS-Installation“ auf der vRealize Automation-Appliance unter `https:// va-hostname.domain.name:5480/install`.
 - b Laden Sie das Installationsprogramm für den Management-Agent herunter und führen Sie es aus.
 - c Starten Sie die Management-Agent-Maschine neu.
 - d Starten Sie das Upgrade auf der virtuellen Appliance neu.

Upgrade des Management-Agents war nicht erfolgreich

Beim Upgrade von vRealize Automation auf 7.2 bis 7.3.x ist das Upgrade des Management Agents nicht erfolgreich.

Problem

Wenn bei einem Failover-Vorfall ein Wechsel zwischen dem primären und dem sekundären Management-Agent-Host stattgefunden hat, ist das Upgrade nicht erfolgreich, weil der erwartete Host beim automatisierten Upgrade-Vorgang nicht gefunden wird. Führen Sie dieses Verfahren auf jedem IaaS-Knoten durch, auf dem der Management-Agent nicht aktualisiert wurde.

Lösung

- 1 Öffnen Sie die Datei „All.log“ im Protokollordner des Management-Agents unter C:\Programme (x86)\VMware\VCAC\Management Agent\Logs\.

Der Speicherort des Installationsordners kann vom Standardspeicherort abweichen.

- 2 Durchsuchen Sie die Protokolldatei nach einer Meldung über eine veraltete oder ausgeschaltete virtuelle Appliance.

Beispiel: INNERE AUSNAHME: System.Net.WebException: Verbindung zum Remoteserver nicht möglich ---> System.Net.Sockets.SocketException: Ein Verbindungsversuch ist fehlgeschlagen, da die verbundene Partei nach einem bestimmten Zeitraum nicht ordnungsgemäß geantwortet hat, oder die eingerichtete Verbindung ist ausgefallen, da der verbundene Host nicht geantwortet hat *IP_Address:5480*

- 3 Bearbeiten Sie die Konfigurationsdatei des Management-Agents unter C:\Programme (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config und ersetzen Sie den vorhandenen Wert „alternativeEndpointaddress“ durch die URL des Endpoints der primären virtuellen Appliance.

Der Speicherort des Installationsordners kann vom Standardspeicherort abweichen.

Beispiel für „alternativeEndpointaddress“ in VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 Starten Sie den Management-Agent-Windows-Dienst neu und überprüfen Sie anhand der Datei All.log, ob er arbeitet.
- 5 Führen Sie das Upgrade-Verfahren auf der primären vRealize Automation-Appliance durch.

Update von vRealize Automation schlägt aufgrund von Standardeinstellungen für die Zeitüberschreitung fehl

Sie können die Zeiteinstellung für Updates erhöhen, wenn die Standardeinstellung für die Synchronisierung von Datenbanken für Ihre Umgebung zu kurz ist.

Problem

Der Zeitüberschreitungswert für den Vcac-Config-Befehl SynchronizeDatabases reicht für bestimmte Umgebungen nicht aus, in denen die Synchronisierung von Datenbanken länger als der Standardwert von 3600 Sekunden dauert.

Die Eigenschaftswerte `cafeTimeoutInSeconds` und `cafeRequestPageSize` in der Datei `Vcac-Config.exe.config` steuern die Kommunikation zwischen der API und dem `Vcac-config.exe`-Hilfsprogramm. Die Datei befindet sich im *Speicherort der IaaS-Installation* `VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config`.

Sie können den standardmäßigen Zeitüberschreitungswert ausschließlich für den Befehl `SynchronizeDatabases` überschreiben, indem Sie einen Wert für diese optionalen Parameter angeben.

Parameter	Kurzname	Beschreibung
<code>--DatabaseSyncTimeout</code>	<code>-dstm</code>	Legt den Zeitüberschreitungswert der HTTP-Anforderung ausschließlich für <code>SynchronizeDatabases</code> in Sekunden fest.
<code>--DatabaseSyncPageSize</code>	<code>-dsps</code>	Legt die Seitengröße der Synchronisierungsanforderung ausschließlich für die Synchronisierung von Reservierungen oder Reservierungsrichtlinien fest. Die Standardeinstellung ist 10.

Wenn diese Parameter in der Datei `Vcac-Config.exe.config` nicht festgelegt sind, verwendet das System den standardmäßigen Zeitüberschreitungswert.

Fehlschlagen des Upgrades von IaaS in einer Hochverfügbarkeitsumgebung

Die Ausführung des IaaS-Upgrades auf einem primären Webserverknoten mit aktiviertem Lastausgleich schlägt fehl. Möglicherweise werden diese Fehlermeldungen angezeigt: "System.Net.WebException: Der Vorgang wurde wegen Zeitüberschreitung abgebrochen" oder "401 - Nicht autorisiert: Zugriff wurde aufgrund von falschen Anmeldedaten verweigert."

Problem

Ein Upgrade von IaaS mit aktiviertem Lastausgleich kann einen vorübergehenden Fehler verursachen. Wenn dieser Fall eintritt, müssen Sie das vRealize Automation-Upgrade erneut mit deaktiviertem Lastausgleich ausführen.

Lösung

- 1 Setzen Sie Ihre Umgebung auf die Snapshots vor dem Upgrade zurück.
- 2 Öffnen Sie eine Remotedesktopverbindung auf dem primären IaaS-Webserver-Knoten.
- 3 Navigieren Sie zur Windows-Host-Datei (`c:\windows\system32\drivers\etc`).
- 4 Öffnen Sie die Host-Datei und fügen Sie die folgende Zeile hinzu, um den Webserver-Lastausgleich zu umgehen.

```
IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn
```

Beispiel:

```
10.10.10.5 vra-iaas-web-lb.domain.com
```

- 5 Speichern Sie die Host-Datei und führen Sie das vRealize Automation-Upgrade erneut aus.

- 6 Wenn das vRealize Automation-Update abgeschlossen ist, öffnen Sie die Host-Datei und entfernen Sie die Zeile, die Sie in Schritt 4 hinzugefügt haben.

Umgehen von Problemen beim Upgrade

Sie können den Upgradevorgang anpassen, um Probleme beim Upgrade zu umgehen.

Lösung

Wenn beim Upgrade Ihrer vRealize Automation-Umgebung Probleme auftreten, verwenden Sie das folgende Verfahren, um den Upgradevorgang durch Auswahl eines der verfügbaren Flags zu ändern.

Verfahren

- 1 Öffnen Sie eine Secure Shell-Verbindung zum Knoten der primären vRealize Automation-Appliance.
- 2 Führen Sie in der Eingabeaufforderung diesen Befehl aus, um die Toggle-Datei zu erstellen:

touch *available_flag*

Beispiel: **touch /tmp/disable-iaas-upgrade**

Tabelle 1-72. Verfügbare Flags

Flag	Beschreibung
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Verhindert das IaaS-Upgrade nach dem Neustart der virtuellen Appliance. ■ Verhindert das Upgrade des Management-Agent. ■ Verhindert die automatische Überprüfung der Voraussetzungen und etwaige Fehlerbehebungen. ■ Verhindert das Beenden von IaaS-Diensten.
/tmp/do-not-upgrade-ma	Verhindert das Upgrade des Management-Agent. Dieses Flag ist geeignet, wenn der Management-Agent manuell aktualisiert wird.
/tmp/skip-prereq-checks	Verhindert die automatische Überprüfung der Voraussetzungen und etwaige Fehlerbehebungen. Dieses Flag ist geeignet, wenn ein Problem bei der automatischen Fehlerbehebung der Voraussetzungen auftritt und die Fehlerbehebung stattdessen manuell durchgeführt werden.
/tmp/do-not-stop-services	Verhindert das Beenden von IaaS-Diensten. Das Upgrade hält die IaaS-Windows-Dienste, wie z. B. den Manager Service, DEM-Instanzen und Agents, nicht an.
/tmp/do-not-upgrade-servers	Verhindert das automatische Upgrade aller IaaS-Serverkomponenten, wie die Datenbank, Website, WAPI, Repository, Model Manager-Daten und Manager Service. Hinweis Dieses Flag verhindert zudem die Aktivierung des automatischen Manager Service-Failover-Modus.
/tmp/do-not-upgrade-dems	Verhindert das DEM-Upgrade.
/tmp/do-not-upgrade-agents	Verhindert das Upgrade des IaaS-Proxy-Agent.

3 Führen Sie die Aufgaben für Ihr ausgewähltes Flag durch.

Tabelle 1-73. Zusätzliche Aufgaben

Flag	Aufgaben
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Aktualisieren Sie den Management-Agent manuell. ■ Wenden Sie alle erforderlichen IaaS-Komponenten manuell an. ■ Halten Sie die IaaS-Dienste manuell an. <ol style="list-style-type: none"> a Melden Sie sich bei Ihrem IaaS-Windows-Server an. b Wählen Sie Start > Verwaltung > Dienste aus. c Halten Sie diese Dienste in der folgenden Reihenfolge an. <p>Hinweis Fahren Sie den IaaS-Windows-Server nicht herunter.</p> <ol style="list-style-type: none"> a Jeder VMware vRealize Automation-Proxy-Agent. b Jeder VMware-DEM-Worker. c Der VMware-DEM-Orchestrator. d Der VMware vCloud Automation Center-Dienst. ■ Starten Sie das IaaS-Upgrade manuell, nachdem das Upgrade der virtuellen Appliance abgeschlossen ist.
/tmp/do-not-upgrade-ma	Aktualisieren Sie den Management-Agent manuell.
/tmp/skip-prereq-checks	Wenden Sie alle erforderlichen IaaS-Komponenten manuell an.
/tmp/do-not-stop-services	<p>Halten Sie die IaaS-Dienste manuell an.</p> <ol style="list-style-type: none"> 1 Melden Sie sich bei Ihrem IaaS-Windows-Server an. 2 Wählen Sie Start > Verwaltung > Dienste aus. 3 Halten Sie diese Dienste in der folgenden Reihenfolge an. <p>Hinweis Fahren Sie den IaaS-Windows-Server nicht herunter.</p> <ol style="list-style-type: none"> a Jeder VMware vRealize Automation-Proxy-Agent. b Jeder VMware-DEM-Worker. c Der VMware-DEM-Orchestrator. d Der VMware vCloud Automation Center-Dienst.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 Greifen Sie auf die Verwaltungskonsole der primären vRealize Automation-Appliance zu und aktualisieren Sie die primäre vRealize Automation-Appliance.

Hinweis Da jedes Flag bis zu seinem Entfernen aktiv bleibt, führen Sie diesen Befehl aus, um Ihr ausgewähltes Flag nach dem Upgrade zu entfernen: `rm /flag_path/flag_name`. Beispiel: `rm /tmp/disable-iaas-upgrade`.

Migrieren auf vRealize Automation 7.4

Sie können mithilfe einer Migration ein paralleles Upgrade Ihrer aktuellen vRealize Automation-Umgebung auf die aktuelle Version durchführen.

Diese Informationen gelten speziell für das Upgrade von vRealize Automation auf Version 7.4 mithilfe der Migration. Informationen zu anderen unterstützten Upgrade-Pfaden finden Sie unter [Aktualisieren von vRealize Automation](#).

Migrieren von vRealize Automation

Sie können ein paralleles Upgrade Ihrer aktuellen vRealize Automation-Umgebung mithilfe einer Migration durchführen.

Bei der Migration werden alle Daten, mit Ausnahme von Mandanten und Identitätsquellen, von Ihrer aktuellen vRealize Automation-Quellumgebung in die Zielbereitstellung der neuesten Version von vRealize Automation verschoben. Darüber hinaus werden bei der Migration alle Daten vom eingebetteten vRealize Orchestrator 7.x auf die Zielbereitstellung verschoben.

Bei der Migration wird die Quellumgebung nur zum Beenden von vRealize Automation-Diensten für das sichere Erfassen und Kopieren der Daten in die Zielumgebung verändert. Je nach Umfang der vRealize Automation-Quelldatenbank kann die Migration zwischen wenigen Minuten bis zu mehreren Stunden dauern.

Sie können Ihre Quellumgebung in eine minimale Bereitstellung oder eine Hochverfügbarkeitsbereitstellung migrieren.

Wenn Sie Ihre Zielumgebung nach der Migration in einer Produktionsumgebung einsetzen möchten, nehmen Sie Ihre Quellumgebung nicht wieder in Betrieb. Änderungen an Ihrer Quellumgebung werden nach der Migration nicht mehr mit der Zielumgebung synchronisiert.

Wenn Ihre Quellumgebung in vCloud Air oder vCloud Director integriert ist oder physische Endpoints aufweist, müssen Sie mithilfe der Migration ein Upgrade durchführen. Im Rahmen der Migration werden diese Endpoints und alle damit verknüpften Elemente aus der Zielumgebung entfernt. Bei der Migration wird außerdem eine Integration einer 6.x-Version von VMware vRealize Application Services aus der Zielumgebung entfernt.

Hinweis Sie müssen zusätzliche Aufgaben ausführen, um Ihre virtuellen vRealize Automation-Maschinen vorzubereiten, bevor Sie die Migration durchführen. Bevor Sie die Migration durchführen, lesen Sie den Knowledgebase-Artikel [51531](#).

Wenn Sie von vRealize Automation 6.2.x auf die neueste Version migrieren, kann dies zu folgenden Problemen führen.

Problem	Lösung
<p>Nach der Migration von vRealize Automation 6.2.x auf die neueste Version werden Katalogelemente, die diese Eigenschaftsdefinitionen verwenden, im Servicekatalog angezeigt, können jedoch nicht angefordert werden.</p> <ul style="list-style-type: none"> ■ Steuerungstypen: Kontrollkästchen oder Verknüpfung. ■ Attribute: Beziehung, reguläre Ausdrücke oder Eigenschaftslayouts. <p>In vRealize Automation 7.x werden in Eigenschaftsdefinitionen diese Elemente nicht mehr verwendet.</p>	<p>Sie müssen die Eigenschaftsdefinitionen neu erstellen oder sie neu konfigurieren, sodass eine vRealize Orchestrator-Skriptaktion anstelle der eingebetteten Steuerungstypen oder Attribute verwendet wird. Weitere Informationen finden Sie unter Katalogelemente werden nach der Migration im Servicekatalog aufgeführt, können aber nicht angefordert werden.</p>
<p>Reguläre Ausdrücke, die zum Definieren von über-/untergeordneten Beziehungen in einem vRealize Automation 6.2.x-Dropdown-Menü verwendet wurden, werden in Version 7.x nicht unterstützt. In Version 6.2.x können Sie reguläre Ausdrücke verwenden, um ein oder mehrere untergeordnete Menüelemente zu definieren, die nur für ein bestimmtes übergeordnetes Menüelement verfügbar sind. Nur diese untergeordneten Menüelemente werden angezeigt, wenn Sie das übergeordnete Menüelement auswählen.</p> <p>Nach der Migration auf Version 7.x werden alle verfügbaren Menüelemente im untergeordneten Dropdown-Menü angezeigt. Dabei spielt es keine Rolle, was im übergeordneten Dropdown-Menü ausgewählt wurde. Um anzuzeigen, dass zuvor definierte dynamische Werte nicht mehr funktionieren, lautet das erste Menüelement im untergeordneten Dropdown-Menü „Warnung! Verwenden Sie vRO-Workflows zum Definieren dynamischer Werte“.</p>	<p>Nach der Migration müssen Sie die Eigenschaftsdefinition zum Wiederherstellen der vorherigen dynamischen Werte neu erstellen. Informationen zum Erstellen einer hierarchischen Beziehung zwischen dem übergeordneten und dem untergeordneten Dropdown-Menü finden Sie unter Verwendung dynamischer Eigenschaftsdefinitionen in vRA 7.2.</p>

Benutzeroberflächen der vRealize Automation -Umgebung

Sie verwenden und verwalten Ihre vRealize Automation-Umgebung mit mehreren Schnittstellen.

Benutzeroberfläche

In diesen Tabellen werden die Schnittstellen beschrieben, die Sie zum Verwalten Ihrer vRealize Automation-Umgebung verwenden

Tabelle 1-74. vRealize Automation Verwaltungskonsole

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die vRealize Automation-Konsole für diese Systemadministrationsaufgaben.</p> <ul style="list-style-type: none"> ■ Mandanten hinzufügen. ■ vRealize Automation-Benutzeroberfläche anpassen. ■ E-Mail-Server konfigurieren. ■ Ereignisprotokolle anzeigen. ■ Konfigurieren Sie vRealize Orchestrator. 	<p>1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance:</p> <p><code>https://vra-va-hostname.domain.name.</code></p> <p>2 Klicken Sie auf vRealize Automation-Konsole.</p> <p>Sie können auch diese URL zum Öffnen der vRealize Automation-Konsole verwenden:</p> <p><code>https://vra-va-hostname.domain.name/vcac</code></p> <p>3 Melden Sie sich an.</p>	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle sein.</p>

Tabelle 1-75. vRealize Automation -Mandantenkonsole. Diese Schnittstelle ist die primäre Benutzeroberfläche, mit der Sie Ihre Dienste und Ressourcen erstellen und verwalten.

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden vRealize Automation für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Neue IT-Dienst-Blueprints anfordern. ■ Cloud- und IT-Ressourcen erstellen und verwalten. ■ Benutzerdefinierte Gruppen erstellen und verwalten. ■ Erstellt und verwaltet Business-Gruppen. ■ Rollen zu Benutzern zuweisen. 	<p>1 Starten Sie einen Browser und geben Sie die URL für Ihren Mandanten mit dem vollqualifizierten Domännennamen der virtuelle Appliance und dem Namen der Mandanten-URL ein.</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name .</code></p> <p>2 Melden Sie sich an.</p>	<p>Sie müssen ein Benutzer mit mindestens einer dieser Rollen sein:</p> <ul style="list-style-type: none"> ■ Anwendungsarchitekt ■ Genehmigungsadministrator ■ Katalog-Administrator ■ Container-Administrator ■ Container-Architekt ■ Health Consumer ■ Infrastrukturarchitekt ■ Sicherer Export, Verbraucher ■ Softwarearchitekt ■ Mandantenadministrator ■ XaaS-Architekt

Tabelle 1-76. Verwaltung der vRealize Automation -Appliance Diese Schnittstelle wird manchmal als „Virtual Appliance Management Interface“ (VAMI) bezeichnet.

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Verwaltung der vRealize Automation-Appliance für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Status der registrierte Dienste anzeigen. ■ Systeminformationen anzeigen und die Appliance neu starten oder herunterfahren. ■ Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit verwalten. ■ Netzwerkstatus anzeigen. ■ Updatestatus anzeigen und Updates installieren. ■ Administrationseinstellungen verwalten. ■ vRealize Automation-Hosteinstellungen verwalten. ■ SSO-Einstellungen verwalten. ■ Lizenzen verwalten. ■ vRealize Automation-Postgres-Datenbank konfigurieren. ■ vRealize Automation-Meldungen konfigurieren. ■ vRealize Automation-Protokollierung konfigurieren. ■ IaaS-Komponenten installieren. ■ Von einer vorhandenen vRealize Automation-Installation migrieren. ■ IaaS-Komponentenzertifikate verwalten. ■ Xenon-Dienst konfigurieren. 	<p>1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code></p> <p>2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance.</p> <p>Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code></p> <p>3 Melden Sie sich an.</p>	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance eingegebene Kennwort.

Tabelle 1-77. vRealize Orchestrator -Client

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden den vRealize Orchestrator-Client für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Aktionen entwickeln. ■ Workflows entwickeln. ■ Richtlinien verwalten. ■ Pakete installieren. ■ Berechtigungen für Benutzer und Benutzergruppen verwalten. ■ Tags an URI-Objekte anhängen. ■ Bestandsliste anzeigen. 	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die vRealize Automation-Begrüßungsseite mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Um die Datei „client.jnlp“ auf Ihren lokalen Computer zu laden, klicken Sie auf vRealize Orchestrator-Client. 3 Klicken Sie mit der rechten Maustaste auf die <code>client.jnlp</code>-Datei und wählen Sie Starten aus. 4 Klicken Sie im Dialogfeld „Möchten Sie fortfahren“ auf Weiter. 5 Melden Sie sich an. 	<p>Sie müssen ein Benutzer mit der Systemadministratorrolle oder Mitglied der Gruppe „vcoadmins“ in den Authentifizierungsanbieter-Einstellungen im vRealize Orchestrator-Control Center sein.</p>

Tabelle 1-78. vRealize Orchestrator Control Center

Zweck	Zugriff	Erforderliche Anmeldeda- ten
<p>Sie verwenden das vRealize Orchestrator Control Center, um die Konfiguration der vRealize Orchestrator-Standardinstanz zu bearbeiten, die in vRealize Automation eingebettet ist.</p>	<ol style="list-style-type: none"> 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation-Appliance mit dem vollqualifizierten Domänennamen für die virtuelle Appliance: <code>https://vra-va-hostname.domain.name.</code> 2 Klicken Sie auf Verwaltung der vRealize Automation-Appliance. Sie können auch diese URL zum Öffnen der Verwaltung der vRealize Automation-Appliance verwenden: <code>https://Vra-va-hostname.domain.name:5480.</code> 3 Melden Sie sich an. 4 Klicken Sie auf vRA-Einstellungen > Orchestrator. 5 Wählen Sie Orchestrator-Benutzeroberfläche aus. 6 Klicken Sie auf Starten. 7 Klicken Sie auf die URL für die Orchestrator-Benutzeroberfläche. 8 Melden Sie sich an. 	<p>Benutzername</p> <ul style="list-style-type: none"> ■ Geben Sie root ein, wenn keine rollenbasierte Authentifizierung konfiguriert ist. ■ Geben Sie Ihren vRealize Automation-Benutzernamen ein, wenn dieser für die rollenbasierte Authentifizierung konfiguriert ist. <p>Kennwort</p> <ul style="list-style-type: none"> ■ Geben Sie das Kennwort ein, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben, wenn die rollenbasierte Authentifizierung nicht konfiguriert ist. ■ Geben Sie das Kennwort für Ihren Benutzernamen ein, wenn Ihr Benutzername für die rollenbasierte Authentifizierung konfiguriert ist.

Tabelle 1-79. Linux-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Sie verwenden die Linux-Befehlszeile auf einem Host, z. B. auf dem Host der vRealize Automation-Appliance Host, für diese Aufgaben.</p> <ul style="list-style-type: none"> ■ Dienste starten oder beenden ■ Konfigurationsdateien bearbeiten ■ Befehle ausführen ■ Daten abrufen 	<p>1 Öffnen Sie auf dem Host der vRealize Automation-Appliance eine neue Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile auf Ihrem lokalen Computer zu öffnen, ist das Starten einer Sitzung auf dem Host mit einer Anwendung, zum Beispiel PuTTY.</p> <p>2 Melden Sie sich an.</p>	<ul style="list-style-type: none"> ■ Benutzername: root ■ Kennwort: Das von Ihnen bei der Bereitstellung der vRealize Automation-Appliance erstellt Kennwort.

Tabelle 1-80. Windows-Befehlszeile

Zweck	Zugriff	Erforderliche Anmeldedaten
<p>Wie können eine Windows-Eingabeaufforderung auf einem Host verwenden z. B. auf dem IaaS-Host, um Skripts ausführen.</p>	<p>1 Melden Sie sich auf dem IaaS-Host bei Windows an.</p> <p>Eine Möglichkeit, sich über Ihren lokalen Computer anzumelden, ist das Starten einer Remote-Desktop-Sitzung.</p> <p>2 Öffnen Sie die Windows-Eingabeaufforderung.</p> <p>Eine Möglichkeit, die Befehlszeile zu öffnen, ist das Klicken mit der rechten Maustaste auf das Startsymbol auf dem Host und die Auswahl von Eingabeaufforderung oder Eingabeaufforderung (Admin).</p>	<ul style="list-style-type: none"> ■ Benutzername: Benutzer mit Administratorrechten. ■ Kennwort: Kennwort des Benutzers.

Voraussetzungen für die Migration

Die Voraussetzungen für die Migration unterscheiden sich je nach Ihrer Zielumgebung.

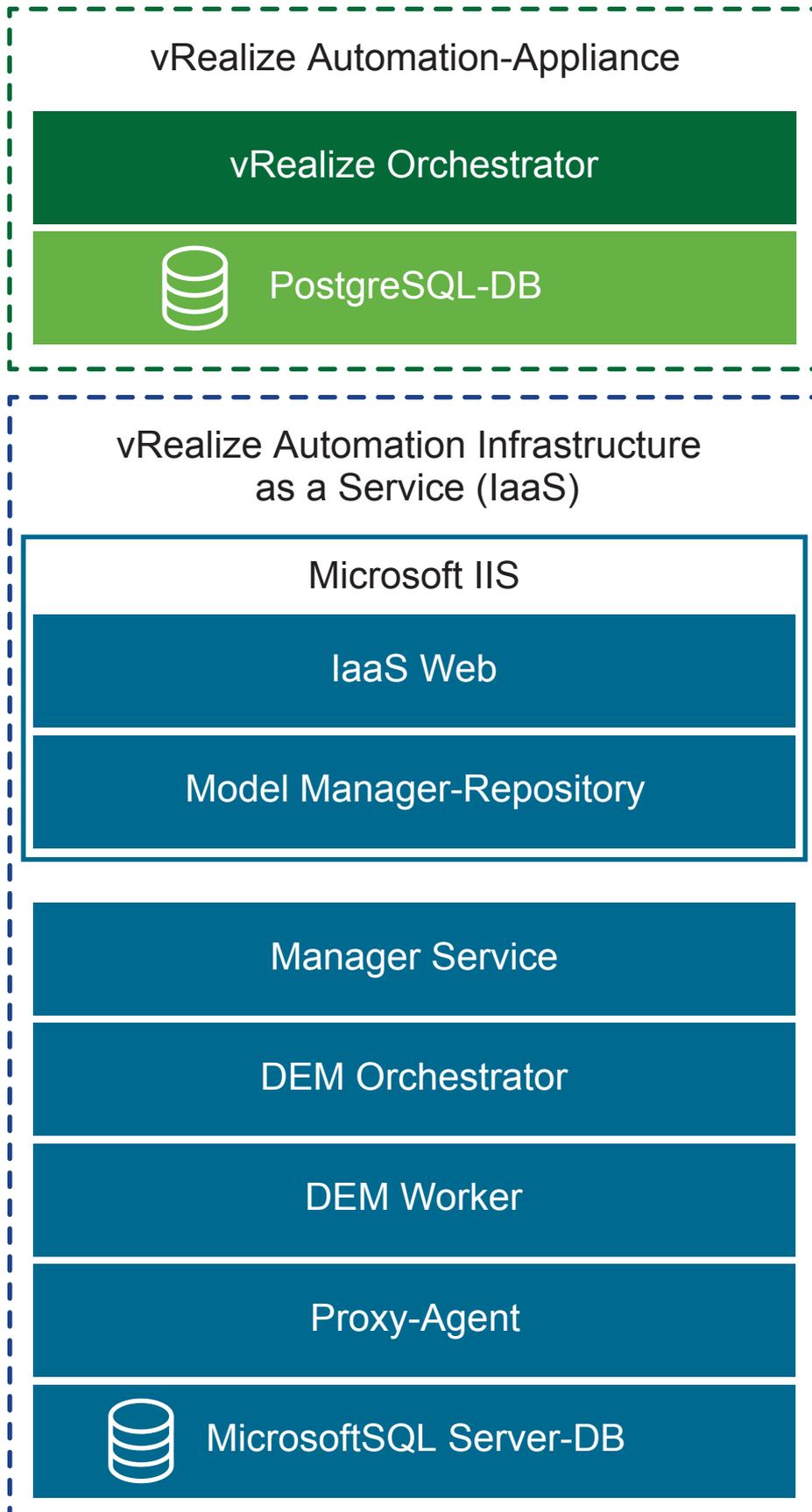
Sie können auf eine Minimalumgebung oder auf eine Hochverfügbarkeitsumgebung migrieren.

Voraussetzungen für die Migration mit einer Minimalumgebung

Stellen Sie eine erfolgreiche Migration in einer minimalen Umgebung sicher, indem Sie diese Voraussetzungen überprüfen.

Minimalbereitstellungen enthalten eine vRealize Automation-Appliance und einen Windows-Server, der die IaaS-Komponenten hostet. In einer Minimalbereitstellung kann sich die SQL Server-Datenbank von vRealize Automation auf demselben IaaS-Windows-Server mit den IaaS-Komponenten oder auf einem separaten Windows-Server befinden.

Abbildung 1-17. vRealize Automation -Minimalbereitstellung



Voraussetzungen

- Stellen Sie sicher, dass Sie über eine neue Zielumgebung für vRealize Automation verfügen.
- Installieren Sie die relevanten Proxy-Agents in der Zielumgebung gemäß diesen Anforderungen.
 - Für vSphere, Hyper-V, Citrix XenServer und Test-Proxy-Agents muss der Name des zieleseitigen Proxy-Agents mit dem Namen des quellseitigen Proxy-Agents übereinstimmen.

Hinweis Führen Sie die folgenden Schritte durch, um einen Agent-Namen zu erhalten.

- 1 Melden Sie sich auf dem IaaS-Host als lokaler Benutzer mit **Administratorrechten** bei Windows an.
- 2 Verwenden Sie Windows Explorer, um zum Installationsverzeichnis des Agent zu wechseln.
- 3 Öffnen Sie die Datei „VRMAgent.exe.config“.
- 4 Suchen Sie unter dem Tag „ServiceConfiguration“ den Wert des Attributs „AgentName“.

-
- Lesen Sie den Knowledgebase-Artikel [51531](#).
 - Für vSphere, Hyper-V, Citrix XenServer und Test-Proxy-Agents muss der Name des zieleseitigen Proxy-Agent-Endpoints mit dem Namen des quellseitigen Proxy-Agent-Endpoints übereinstimmen.
 - Erstellen Sie in der Zielumgebung keinen Endpoint für vSphere, Hyper-V, Citrix XenServer oder Test-Proxy-Agents.
 - Überprüfen Sie die Versionsnummern der vRealize Automation-Komponenten auf der zieleseitigen vRealize Automation-Appliance.
 - a Melden Sie sich bei der Verwaltung der zieleseitigen vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der zieleseitigen vRealize Automation-Appliance eingegeben haben.
 - b Wählen Sie **vRA-Einstellungen > Cluster** aus.
 - c Klicken Sie auf das Dreieck, um die Datensätze mit den Host- bzw. Knotennamen zu erweitern.

Stellen Sie sicher, dass die Versionsnummern der vRealize Automation IaaS-Komponenten übereinstimmen.
 - Stellen Sie sicher, dass es sich bei der Microsoft SQL Server-Zielversion für die IaaS-vRealize Automation-Zieldatenbank um 2012, 2014 oder 2016 handelt.
 - Stellen Sie sicher, dass Port 22 zwischen den Quell- und Zielumgebungen von vRealize Automation geöffnet ist. Port 22 ist erforderlich, um Secure Shell (SSH) -Verbindungen zwischen quell- und zieleseitigen virtuellen Appliances herzustellen.
 - Vergewissern Sie sich, dass die Endpoint-vCenter-Instanz über ausreichende Ressourcen verfügt, um die Migration abzuschließen.
 - Vergewissern Sie sich, dass die Systemzeit der vRealize Automation-Zielumgebung zwischen Cloud- und IaaS-Komponenten synchronisiert ist.

- Stellen Sie sicher, dass auf jedem IaaS-Serverknoten in der Zielumgebung mindestens Java SE Runtime Environment (JRE) 8, 64 Bit, Update 161 oder höher installiert ist. Stellen Sie nach dem Installieren von JRE sicher, dass die Umgebungsvariable JAVA_HOME auf die auf jedem IaaS-Knoten installierte Java-Version verweist. Überarbeiten Sie nötigenfalls den Pfad.
- Stellen Sie sicher, dass für jeden IaaS-Knoten PowerShell 3.0 oder höher installiert wurde.
- Stellen Sie sicher, dass die vRealize Automation-Quell- und Zielumgebungen ausgeführt werden.
- Stellen Sie sicher, dass in der vRealize Automation-Quellumgebung keine Benutzer- oder Bereitstellungsaktivitäten ausgeführt werden.
- Vergewissern Sie sich, dass die Antiviren- oder Sicherheitssoftware, die auf den IaaS-Knoten in der möglicherweise mit dem Betriebssystem und dessen Komponenten interagierenden vRealize Automation-Zielumgebung korrekt konfiguriert oder deaktiviert ist.
- Stellen Sie sicher, dass der IaaS-Webdienst und der Modellmanager aufgrund ausstehender Updates der Windows-Installation nicht neu gestartet werden müssen. Ausstehende Updates können die Migration daran hindern, den World Wide Web Publishing-Dienst zu starten oder zu beenden.

Nächste Schritte

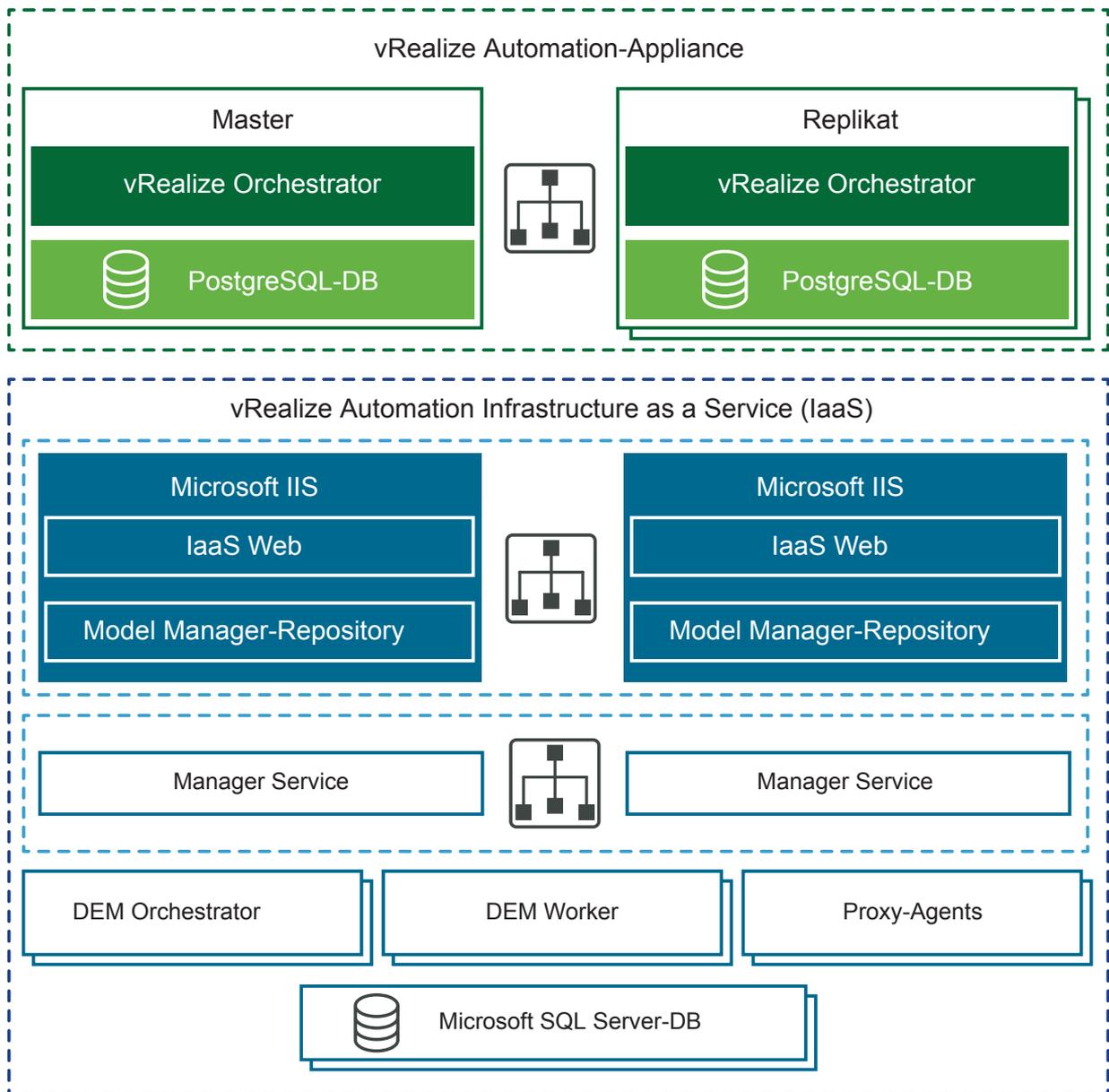
[Aufgaben vor der Migration.](#)

Voraussetzungen für die Migration in einer Hochverfügbarkeitsumgebung

Sie können den Erfolg der Migration in eine Hochverfügbarkeitsumgebung gewährleisten, indem Sie die folgenden Voraussetzungen beachten.

Hochverfügbarkeitsumgebungen können unterschiedliche Größen aufweisen. Eine grundlegende verteilte Bereitstellung kann zur Verbesserung von vRealize Automation führen, indem IaaS-Komponenten einfach auf separaten Windows-Servern gehostet werden. Viele Hochverfügbarkeitsumgebungen gehen mit redundanten Appliances, redundanten Servern und sogar Lastausgleichsdiensten für noch mehr Kapazität noch weiter. Große, verteilte Bereitstellungen bieten bessere Skalierung, Hochverfügbarkeit und Notfallwiederherstellung.

Abbildung 1-18. vRealize Automation -Hochverfügbarkeitsumgebung



Voraussetzungen

- Stellen Sie sicher, dass Sie über eine neue Zielinstallation von vRealize Automation mit einer virtuellen Master- und Replikat-Appliance mit konfigurierter Hochverfügbarkeit verfügen. Weitere Informationen finden Sie unter [Erwägungen zur Konfiguration der Hochverfügbarkeit \(HA, High Availability\) von vRealize Automation](#).
- Stellen Sie sicher, dass alle virtuellen vRealize Automation-Appliances dasselbe Kennwort für den Root-Benutzer verwenden.
- Installieren Sie die relevanten Proxy-Agents in der Zielumgebung gemäß diesen Anforderungen.
 - Für vSphere, Hyper-V, Citrix XenServer und Test-Proxy-Agents muss der Name des zieleseitigen Proxy-Agents mit dem Namen des quellseitigen Proxy-Agents übereinstimmen.

Hinweis Führen Sie die folgenden Schritte durch, um einen Agent-Namen zu erhalten.

- 1 Melden Sie sich auf dem IaaS-Host als lokaler Benutzer mit **Administratorrechten** bei Windows an.
 - 2 Verwenden Sie Windows Explorer, um zum Installationsverzeichnis des Agent zu wechseln.
 - 3 Öffnen Sie die Datei „VRMAgent.exe.config“.
 - 4 Suchen Sie unter dem Tag „ServiceConfiguration“ den Wert des Attributs „AgentName“.
-
- Für vSphere, Hyper-V, Citrix XenServer und Test-Proxy-Agents muss der Name des zieleseitigen Proxy-Agent-Endpoints mit dem Namen des quellseitigen Proxy-Agent-Endpoints übereinstimmen.
 - Erstellen Sie in der Zielumgebung keinen Endpoint für vSphere, Hyper-V, Citrix XenServer oder Test-Proxy-Agents.
- Überprüfen Sie die Versionsnummern der vRealize Automation-Komponenten auf der zieleseitigen vRealize Automation-Appliance.
 - a Starten Sie in Ihrer vRealize Automation-Zielumgebung einen Browser und wechseln Sie zur Verwaltungskonsole der vRealize Automation-Appliance unter `https:// vra-va-hostname.domain.name:5480`.
 - b Melden Sie sich mit dem beim Bereitstellen der Appliance eingegebenen Benutzernamen „root“ und dem zugehörigen Kennwort an.
 - c Wählen Sie **vRA-Einstellungen > Cluster** aus.
 - d Klicken Sie auf die Schaltfläche zum Erweitern, um die Anzeige der Host-/Knotenname-Datensätze zu erweitern und die Komponenten sichtbar zu machen.

Stellen Sie sicher, dass die Versionsnummern der vRealize Automation-Komponenten auf allen virtuellen Appliance-Knoten übereinstimmen.

Stellen Sie sicher, dass die Versionsnummern der vRealize Automation-IaaS-Komponenten auf allen IaaS-Knoten übereinstimmen.
 - Lesen Sie den Knowledgebase-Artikel [51531](#).

- Führen Sie diese Schritte aus, um den Datenverkehr ausschließlich zum Master-Knoten zu leiten.
 - a Deaktivieren Sie alle redundanten Knoten.
 - b Entfernen Sie die Integritätsüberwachungen für diese Elemente gemäß den Anweisungen in der Dokumentation zu Ihrem Lastausgleichsdienst:
 - Virtuelle vRealize Automation-Appliance
 - IaaS-Website
 - IaaS Manager Service
- Stellen Sie sicher, dass es sich bei der Microsoft SQL Server-Zielversion für die IaaS-vRealize Automation-Zieldatenbank um 2012, 2014 oder 2016 handelt.
- Stellen Sie sicher, dass Port 22 zwischen den Quell- und Zielumgebungen von vRealize Automation geöffnet ist. Port 22 ist erforderlich, um Secure Shell (SSH) -Verbindungen zwischen quell- und ziel-seitigen virtuellen Appliances herzustellen.
- Vergewissern Sie sich, dass die Endpoint-vCenter-Instanz über ausreichende Ressourcen verfügt, um die Migration abzuschließen.
- Vergewissern Sie sich, dass Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst vom Standardwert auf mindestens 10 Minuten geändert haben.
- Vergewissern Sie sich, dass die Systemzeit der vRealize Automation-Zielumgebung zwischen Cafe- und IaaS-Komponenten synchronisiert ist.
- Vergewissern Sie sich, dass die IaaS-Webdienst- und Model Manager-Knoten in der Zielumgebung über die passende Java-Laufzeitumgebung verfügen. Java SE Runtime Environment (JRE) 8, 64 Bit, Update 161 oder höher muss installiert sein. Vergewissern Sie sich, dass die Systemvariable JAVA_HOME auf die Java-Version verweist, die Sie auf jedem IaaS-Knoten installiert haben. Überarbeiten Sie nötigenfalls den Pfad.
- Stellen Sie sicher, dass für jeden IaaS-Knoten PowerShell 3.0 oder höher installiert wurde.
- Stellen Sie sicher, dass die vRealize Automation-Quell- und Zielumgebungen ausgeführt werden.
- Stellen Sie sicher, dass in der vRealize Automation-Quellumgebung keine Benutzer- oder Bereitstellungsaktivitäten ausgeführt werden.
- Vergewissern Sie sich, dass die Antiviren- oder Sicherheitssoftware, die auf den IaaS-Knoten in der möglicherweise mit dem Betriebssystem und dessen Komponenten interagierenden vRealize Automation-Zielumgebung korrekt konfiguriert oder deaktiviert ist.
- Stellen Sie sicher, dass der IaaS-Webdienst und der Modellmanager aufgrund ausstehender Updates der Windows-Installation nicht neu gestartet werden müssen. Ausstehende Updates können die Migration daran hindern, den World Wide Web Publishing-Dienst zu starten oder zu beenden.

Nächste Schritte

[Aufgaben vor der Migration.](#)

Aufgaben vor der Migration

Vor einer Migration müssen Sie mehrere vorbereitende Aufgaben durchführen.

Die Aufgaben der Migration Ihrer vRealize Automation-Quellumgebung auf Ihre vRealize Automation-Ziellumgebung richten sich nach Ihrer jeweiligen Quellumgebung.

Überprüfen von Änderungen, die durch die Migration von vRealize Automation 6.2.x auf 7.x eingeführt werden

vRealize Automation 7 und höher führt während und nach dem Upgrade-Vorgang verschiedene funktionale Änderungen ein. Überprüfen Sie diese Änderungen, bevor Sie Ihre vRealize Automation 6.2.x-Bereitstellung auf die neueste Version aktualisieren.

Weitere Informationen zu den Unterschieden zwischen vRealize Automation 6.2.x und 7.x finden Sie unter [Überlegungen zum Upgrade auf diese vRealize Automation-Version](#) in *Upgrade von vRealize Automation 6.2.5 auf 7.4*.

Hinweis Das vRealize Production Test Upgrade Assist-Tool analysiert Ihre vRealize Automation 6.2.x-Umgebung hinsichtlich jeder Funktionskonfiguration, die Upgrade-Probleme verursachen kann, und überprüft, ob Ihre Umgebung für das Upgrade bereit ist. Um dieses Tool und die zugehörige Dokumentation herunterzuladen, navigieren Sie zur Downloadseite für das [VMware vRealize Production Test Tool](#).

Nach der Migration von vRealize Automation 6.2.x auf die neueste Version werden Katalogelemente, die diese Eigenschaftsdefinitionen verwenden, im Servicekatalog angezeigt, können jedoch nicht angefordert werden.

- Steuerungstypen: Kontrollkästchen oder Verknüpfung.
- Attribute: Beziehung, reguläre Ausdrücke oder Eigenschaftslayouts.

In vRealize Automation 7.x werden in Eigenschaftsdefinitionen diese Elemente nicht mehr verwendet. Sie müssen die Eigenschaftsdefinitionen neu erstellen oder sie neu konfigurieren, sodass eine vRealize Orchestrator-Skriptaktion anstelle der eingebetteten Steuerungstypen oder Attribute verwendet wird. Weitere Informationen finden Sie unter [Katalogelemente werden nach der Migration im Servicekatalog aufgeführt, können aber nicht angefordert werden](#).

Anwenden des Software-Agent-Patches

Vor der Migration von vRealize Automation 7.1 oder 7.3 zu 7.4 müssen Sie einen Hotfix auf die Quell-Appliance anwenden, damit Sie ein Upgrade der Software-Agents auf TLS 1.2 durchführen können.

Das Transport Layer Security (TLS)-Protokoll bietet Datenintegrität zwischen Ihrem Browser und vRealize Automation. Mit diesem Hotfix ist ein Upgrade der Software-Agents in Ihrer Quellumgebung auf TLS 1.2 möglich. Dieses Upgrade gewährleistet das höchste Sicherheitsniveau und ist für vRealize Automation 7.1 oder 7.3 erforderlich. Jede Version verfügt über einen eigenen Hotfix.

Voraussetzungen

Eine vRealize Automation 7.1- oder 7.3-Quellumgebung, die ausgeführt wird.

Verfahren

- ◆ Wenden Sie diesen Hotfix auf Ihre vRealize Automation 7.1- oder 7.3-Quell-Appliance an, bevor Sie zu 7.4 migrieren. Weitere Informationen finden Sie im [Knowledgebase-Artikel 52897](#).

Nächste Schritte

[Ändern der DoDeletes-Einstellung im vSphere-Agent in „False“](#).

Ändern der DoDeletes-Einstellung im vSphere -Agent in „False“

Wenn Sie von einer vRealize Automation 6.2.x-Umgebung migrieren, müssen Sie den DoDeletes-Wert vor der Migration von **true** in **false** auf Ihrem vSphere-Zielagent ändern.

Voraussetzungen

Schließen Sie die Voraussetzungen für die Migration ab.

Verfahren

- 1 Ändern Sie den DoDeletes-Wert in **false**.

Hiermit wird das Löschen der virtuellen Maschinen aus der Quellumgebung verhindert. Die Quell- und Zielumgebungen werden gleichzeitig ausgeführt. Nach der Validierung der Produktionsmigration können unter Umständen Lease-Diskrepanzen auftreten.

- 2 Legen Sie den DoDeletes-Wert auf **true** fest, nachdem die Produktionsmigration überprüft und die Quellumgebung heruntergefahren wurde.
- 3 Befolgen Sie die Schritte in der Vorgehensweise zum [Konfigurieren des vSphere-Agents](#), um DoDeletes auf **false** festzulegen.

Nächste Schritte

[Vorbereiten von virtuellen vRealize Automation-Maschinen für die Migration](#).

Überprüfen der Vorlagen in Ihrer vRealize Automation 6.x-Quellumgebung

Vor der Migration von vRealize Automation 6.x auf 7.4 müssen Sie die VM-Vorlagen überprüfen, um sicherzustellen, dass jede Vorlage eine Einstellung für die Mindestgröße des Arbeitsspeichers von mindestens 4 MB aufweist.

Wenn Sie in Ihrer vRealize Automation 6.x-Quellumgebung eine VM-Vorlage mit weniger als 4 MB Arbeitsspeicher haben, schlägt die Migration fehl. Führen Sie dieses Verfahren durch, um festzustellen, ob Blueprints in der 6.x-Quellumgebung weniger als 4 MB Arbeitsspeicher haben.

Voraussetzungen

Sie migrieren von vRealize Automation 6.x auf 7.4.

Verfahren

- 1 Melden Sie sich bei der primären vRealize Automation-Appliance über SSH als **root** an.

Wenn vRealize Orchestrator extern ist, melden Sie sich bei der Orchestrator-Host-Maschine an.

2 Wechseln Sie in den PostgreSQL-Datenordner auf dem primären Host unter `/var/vmware/vpostgres/current/pgdata/`.

3 Führen Sie dieses Skript aus, um zu überprüfen, ob es Blueprints mit einem Arbeitsspeicher von weniger als 4 MB gibt.

```
select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and MemoryMB < 4;
```

wobei vCAC der Datenbankname ist.

4 Wenn das Skript Blueprints mit einem Arbeitsspeicher von weniger als 4 MB findet, führen Sie dieses Skript aus, um den Arbeitsspeicher auf mindestens 4 MB zu aktualisieren.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

wobei vCAC der Datenbankname ist.

Nächste Schritte

[Vorbereiten von virtuellen vRealize Automation-Maschinen für die Migration.](#)

Vorbereiten von virtuellen vRealize Automation -Maschinen für die Migration

Bekannte Probleme mit der Migration von virtuellen vRealize Automation 6.2.x-Maschinen können nach der Migration zu Problemen führen.

Sie müssen den [KnowledgeBase-Artikel 000051531](#) durchlesen und alle relevanten Fixes für Ihre Umgebungen vor der Migration durchführen.

Nächste Schritte

[Sammeln von für die Migration erforderlichen Informationen.](#)

Sammeln von für die Migration erforderlichen Informationen

Verwenden Sie diese Tabellen, um Informationen aufzuzeichnen, die Sie für die Migration Ihrer Quell- und Zielumgebungen benötigen.

Voraussetzungen

Schließen Sie die Prüfung der Voraussetzungen für Ihre Situation ab.

- [Voraussetzungen für die Migration mit einer Minimalumgebung.](#)
- [Voraussetzungen für die Migration in einer Hochverfügbarkeitsumgebung.](#)

Tabelle 1-81. Quellseitige vRealize Automation -Appliance

Option	Beschreibung	Wert
Hostname	Melden Sie sich bei der Verwaltungskonsole der quellseitigen vRealize Automation-Appliance an. Suchen Sie den Hostnamen auf der Registerkarte System . Der Hostname muss ein vollqualifizierter Domänenname (FQDN) sein.	
Root-Benutzername	root	
Root-Kennwort	Das bei der Bereitstellung der quellseitigen vRealize Automation-Appliance eingegebene Root-Kennwort.	
Speicherort des Migrationspakets	Pfad zu einem vorhandenen Verzeichnis auf der Quell-Appliance von vRealize Automation 6.2.x oder 7.x, auf der das Migrationspaket erstellt wird. Der verfügbare Speicherplatz in dem Verzeichnis muss doppelt so groß sein wie die Größe der vRealize Automation-Datenbank. Der Standardspeicherort ist /storage.	

Tabelle 1-82. Zielseitige vRealize Automation -Appliance

Option	Beschreibung	Wert
Root-Benutzername	root	
Root-Kennwort	Das bei der Bereitstellung der zielseitigen vRealize Automation-Appliance eingegebene Root-Kennwort.	
Standardmandant	vsphere.local	
Administratorbenutzername	Administrator	
Administratorkennwort	Kennwort des Benutzers administrator@vsphere.local, das Sie bei der Bereitstellung der vRealize Automation-Zielumgebung eingegeben haben.	

Tabelle 1-83. IaaS -Zieldatenbank

Option	Beschreibung	Wert
Datenbankserver	Speicherort der Microsoft SQL Server-Instanz, auf der sich die geklonte Datenbank befindet. Wenn es sich um eine benannte Instanz und einen nicht standardmäßigen Port handelt, verwenden Sie das Format SERVER,PORT\INSTANZNAME.	
Geklonter Datenbankname	Name der vRealize Automation 6.2.x/7.x IaaS Microsoft SQL-Quelldatenbank, die für die Migration geklont wurde.	
Authentifizierungsmodus	Wählen Sie entweder Windows oder SQL Server aus. Bei Auswahl von „SQL Server“ müssen Sie einen Anmeldenamen und ein Kennwort eingeben.	

Tabelle 1-83. IaaS -Zioldatenbank (Fortsetzung)

Option	Beschreibung	Wert
Anmeldename	Anmeldename für den SQL Server-Benutzer, der über die Rolle „db_owner“ für die geklonte IaaS Microsoft SQL-Datenbank verfügt.	
Kennwort	Kennwort für den SQL Server-Benutzer.	
Ursprünglicher Verschlüsselungsschlüssel	Ursprünglicher Verschlüsselungsschlüssel, den Sie aus der Quellumgebung abrufen. Siehe Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung .	
Neue Passphrase	Eine Reihe von Wörtern, die zur Generierung eines neuen Verschlüsselungsschlüssels verwendet werden. Sie verwenden diese Passphrase jedes Mal, wenn Sie eine neue IaaS-Komponente in der vRealize Automation-Zielumgebung installieren.	

Nächste Schritte

[Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung.](#)

Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation -Quellumgebung

Während des Migrationsvorgangs müssen Sie den Verschlüsselungsschlüssel aus der vRealize Automation-Quellumgebung eingeben.

Voraussetzungen

Stellen Sie sicher, dass Sie auf der virtuellen Maschine des aktiven Manager Service-Hosts in Ihrer Quellumgebung über Administratorrechte verfügen.

Verfahren

- 1 Öffnen Sie die Eingabeaufforderung als Administrator auf der virtuellen Maschine, die den aktiven Manager Service in der Quellumgebung hostet, und geben Sie folgenden Befehl ein.

```
"C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config" -v
```

Wenn sich Ihr Installationsverzeichnis nicht am Standardspeicherort C:\Programme (x86)\VMware\vCAC befindet, bearbeiten Sie den Pfad so, dass er Ihrem eigentlichen Installationsverzeichnis entspricht.

- 2 Speichern Sie den Schlüssel, der nach Ausführung des Befehls angezeigt wird.

Der Schlüssel ist eine lange Zeichenfolge, die der Zeichenfolge im nachstehenden Beispiel ähnelt:
NRH+f/BlnCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.

Nächste Schritte

- Wenn Sie von einer vRealize Automation 6.2.x-Umgebung migrieren: [Hinzufügen aller Mandanten aus der vRealize Automation-Quellumgebung zur Zielumgebung](#).
- Wenn Sie von einer vRealize Automation 7.x-Umgebung migrieren: [Auflisten von Mandanten- und IaaS-Administratoren aus der vRealize Automation 6.2.x-Quellumgebung](#).

Auflisten von Mandanten- und IaaS-Administratoren aus der vRealize Automation 6.2.x-Quellumgebung

Bevor Sie eine vRealize Automation 6.2.x-Umgebung migrieren, müssen Sie eine Liste der Mandanten- und IaaS-Administratoren für jeden Mandanten erstellen.

Führen Sie das folgende Verfahren für jeden Mandanten in der quellseitigen vRealize Automation-Konsole durch.

Hinweis Wenn Sie von einer vRealize Automation 7.x-Umgebung migrieren, müssen Sie dieses Verfahren nicht durchführen.

Voraussetzungen

Melden Sie sich bei der quellseitigen vRealize Automation-Konsole als **Administrator** mit dem Kennwort an, das Sie bei der Bereitstellung der quellseitigen vRealize Automation-Appliance eingegeben haben.

Hinweis In einer Hochverfügbarkeitsumgebung öffnen Sie die Konsole mithilfe des vollqualifizierten Domainennamens des Lastausgleichs der quellseitigen virtuellen Appliance: `https://vra-va-lb-hostname.domain.name/vcac`.

Verfahren

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf einen Mandantennamen.
- 3 Klicken Sie auf **Administratoren**.
- 4 Erstellen Sie eine Liste der Benutzernamen der einzelnen Mandanten- und IaaS-Administratoren.
- 5 Klicken Sie auf **Abbrechen**.

Nächste Schritte

[Hinzufügen aller Mandanten aus der vRealize Automation-Quellumgebung zur Zielumgebung](#).

Hinzufügen aller Mandanten aus der vRealize Automation -Quellumgebung zur Zielumgebung

Sie müssen Mandanten in der Zielumgebung unter Verwendung der Namen der einzelnen Mandanten in der Quellumgebung hinzufügen.

Für eine erfolgreiche Migration ist es erforderlich, jeden Mandanten aus der Quellumgebung in der Zielumgebung zu erstellen. Zudem müssen Sie für jeden Mandanten, den Sie hinzufügen, eine mandantenspezifische Zugriffs-URL mit dem Namen der Mandanten-URL aus der Quellumgebung verwenden. Wenn es in der Quellumgebung nicht genutzte Mandanten gibt, die Sie nicht migrieren möchten, löschen Sie sie vor der Migration aus der Quellumgebung.

Hinweis Durch die Validierung der Migration wird sichergestellt, dass das Zielsystem mindestens über die gleichen in der Quelle konfigurierten Mandanten verfügt, die zur Erfüllung der Voraussetzungen erforderlich sind. Bei der Validierung werden die Mandanten verglichen. Dies geschieht auf der Grundlage der URL-Namen der Mandanten (Groß- und Kleinschreibung beachten), nicht der Mandantennamen.

Führen Sie diesen Vorgang für jeden Mandanten in der Quellumgebung aus.

- Bei der Migration von einer vRealize Automation 6.2.x-Umgebung migrieren Sie Ihre vorhandenen SSO2-Mandanten und Identitätsquellen in der Quellumgebung auf den VMware Identity Manager in der Zielumgebung.
- Bei der Migration von einer vRealize Automation 7.x-Umgebung migrieren Sie Ihre vorhandenen VMware Identity Manager-Mandanten und Identitätsquellen in der Quellumgebung auf den VMware Identity Manager in der Zielumgebung.

Voraussetzungen

- [Sammeln von für die Migration erforderlichen Informationen.](#)
- Melden Sie sich bei der zieleitigen vRealize Automation-Konsole als **Administrator** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Ziel-Appliance eingegeben haben.

Hinweis Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domänennamens des Lastausgleichsdiensts der zieleitigen virtuellen Appliance:
`https://vra-va-lb-hostname.domain.name/vcac.`

Verfahren

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie im Textfeld **Name** einen Mandantennamen ein, der einem Mandantennamen in der Quellumgebung entspricht.

Wenn der Mandantennamen in der Quellumgebung zum Beispiel „DEVTenant“ lautet, geben Sie **DEVTenant** ein.

- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.

- 5 Geben Sie im Textfeld **URL-Name** einen Mandanten-URL-Namen ein, der dem Mandanten-URL-Namen der Quellumgebung entspricht.

Mit dem URL-Namen wird ein mandantenspezifischer Bezeichner an die vRealize Automation-Konsolen-URL angefügt.

Wenn der URL-Name für DEVTenant in der Quellumgebung zum Beispiel „dev“ lautet, geben Sie **dev** ein, um die URL `https://vra-va-hostname.domain.name/vcac/org/dev` zu erstellen.

- 6 (Optional) Geben Sie in das Textfeld **E-Mail des Kontakts** eine E-Mail-Adresse ein.
- 7 Klicken Sie auf **Erstellen und Weiter**.

Nächste Schritte

[Erstellen eines Administrators für jeden hinzugefügten Mandanten.](#)

Erstellen eines Administrators für jeden hinzugefügten Mandanten

Sie müssen für jeden Mandanten, den Sie zur Zielumgebung hinzugefügt haben, einen Administrator erstellen. Sie erstellen einen Administrator, indem Sie ein lokales Benutzerkonto erstellen und diesem Mandantenadministratorrechte zuweisen.

Führen Sie diesen Vorgang für jeden Mandanten in der Zielumgebung aus.

Voraussetzungen

- [Hinzufügen aller Mandanten aus der vRealize Automation-Quellumgebung zur Zielumgebung.](#)
- Melden Sie sich bei der zieleitigen vRealize Automation-Konsole als **Administrator** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Ziel-Appliance eingegeben haben.

Hinweis Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domännennamens des Lastausgleichsdiensts der zieleitigen virtuellen Appliance:
`https://vra-va-lb-hostname.domain.name/vcac.`

Verfahren

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf einen Mandanten, den Sie hinzugefügt haben.
Klicken Sie zum Beispiel für DEVTenant auf **DEVTenant**.
- 3 Klicken Sie auf **Lokale Benutzer**.
- 4 Klicken Sie auf das Symbol **Neu (+)**.
- 5 Geben Sie unter **Benutzerdetails** die angeforderten Informationen zum Erstellen eines lokalen Benutzerkontos ein, um die Mandantenadministratorrolle zuzuweisen.
Der lokale Benutzername muss im lokalen Standardverzeichnis „vsphere.local“ eindeutig sein.
- 6 Klicken Sie auf **OK**.
- 7 Klicken Sie auf **Administratoren**.

- 8 Geben Sie den lokalen Benutzernamen im Suchfeld **Mandantenadministratoren** ein und drücken Sie die Eingabetaste.
- 9 Klicken Sie in den Suchergebnissen auf den entsprechenden Namen, um den Benutzer zur Liste der Mandantenadministratoren hinzuzufügen.
- 10 Klicken Sie auf **Fertig stellen**.
- 11 Melden Sie sich von der Konsole ab.

Nächste Schritte

- Für eine Minimalbereitstellung: [Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration mit einer Minimalumgebung](#)
- Für eine Hochverfügbarkeitsbereitstellung: [Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration auf eine Hochverfügbarkeitsumgebung](#)

Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration mit einer Minimalumgebung

Bevor Sie Ihre Benutzer und Gruppen in eine Minimalbereitstellung von vRealize Automation importieren, müssen Sie das zweiseitige vRealize Automation mit Ihrem Active Directory-Link verbinden.

Führen Sie diesen Vorgang für jeden Mandanten durch. Wenn ein Mandant mehrere Active Directories besitzt, führen Sie diesen Vorgang für jedes Active Directory durch, das der Mandant verwendet.

Voraussetzungen

- [Erstellen eines Administrators für jeden hinzugefügten Mandanten](#).
- Überprüfen Sie, ob Sie über Zugriffsberechtigungen für das Active Directory verfügen.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Verzeichnisse** aus.
- 2 Klicken Sie auf das Symbol **Verzeichnis hinzufügen** (+) und wählen Sie **Active Directory über LDAP/IWA hinzufügen** aus.
- 3 Geben Sie Ihre Active Directory-Kontoeinstellungen ein.
 - ◆ Für nicht-native Active Directories

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie Active Directory über LDAP aus, wenn ein nicht-natives Active Directory verwendet wird.
Dieses Verzeichnis unterstützt den DNS-Dienstspeicherort	Deaktivieren Sie diese Option.
Basis-DN	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: cn=users,dc=rainpole,dc=local .

Option	Beispieleingabe
Bind-DN	Geben Sie den vollständigen definierten Namen (DN, Distinguished Name), einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Beispiel: cn=config_admin infra,cn=users,dc=rainpole,dc=local .
Bind-DN-Kennwort	Geben Sie das Active Directory-Kennwort für das Konto ein, das nach Benutzern suchen kann, und klicken Sie auf Testverbindung , um die Verbindung zum konfigurierten Verzeichnis zu testen.

◆ Für native Active Directories

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie Active Directory (Integrierte Windows-Authentifizierung) aus, wenn „Natives Active Directory“ verwendet wird.
Domänenname	Geben Sie den Namen der Domäne ein, der beigetreten werden soll.
Benutzername des Domänenadministrators	Geben Sie den Benutzernamen für den Domänenadministrator ein.
Kennwort des Domänenadministrators	Geben Sie das Kennwort für den Domänenadministrator ein.
Bind-Benutzer-UPN	Geben Sie als Benutzernamen die E-Mail-Adresse des Benutzers ein, der die Domäne authentifizieren kann.
Bind-DN-Kennwort	Geben Sie das Kennwort des Active Directory-Bind-Kontos für das Konto ein, das nach Benutzern suchen kann.

4 Klicken Sie auf **Speichern und weiter**.

Unter **Domänen auswählen** wird eine Liste der Domänen angezeigt.

5 Übernehmen Sie die Einstellung für die Standarddomäne und klicken Sie auf **Weiter**.

6 Überprüfen Sie, ob die Attributnamen den richtigen Active Directory-Attributen zugeordnet sind, und klicken Sie auf **Weiter**.

7 Wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen.

a Klicken Sie auf das Symbol **Neu (+)**.

b Geben Sie die Benutzerdomäne ein und klicken Sie auf **Gruppen suchen**.

Geben Sie beispielsweise **dc=vcac,dc=local** ein.

c Um die Gruppen zur Synchronisierung zu wählen, klicken Sie auf **Auswählen** und **Weiter**.

d Wählen Sie unter **Benutzer auswählen** die Benutzer aus, die synchronisiert werden sollen, und klicken Sie auf **Weiter**.

Fügen Sie nur Benutzer und Gruppen hinzu, die vRealize Automation verwenden müssen. Wählen Sie **Geschachtelte Gruppen synchronisieren** nicht aus, es sei denn, alle Gruppen in der geschachtelten Gruppe müssen vRealize Automation verwenden.

- 8 Überprüfen Sie die Benutzer und Gruppen, die mit dem Verzeichnis synchronisiert werden, und klicken Sie auf **Verzeichnis synchronisieren**.

Für die Verzeichnissynchronisierung wird einige Zeit benötigt. Der Prozess wird im Hintergrund ausgeführt.

Nächste Schritte

[Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation-Quellumgebung](#)

Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration auf eine Hochverfügbarkeitsumgebung

Bevor Sie Ihre Benutzer und Gruppen in eine vRealize Automation-Hochverfügbarkeitsumgebung importieren, müssen Sie eine Verbindung zu Ihrem Active Directory-Link herstellen.

- Führen Sie die Schritte 1 bis 8 für jeden Mandanten durch. Wenn ein Mandant mehrere Active Directories besitzt, führen Sie diesen Vorgang für jedes Active Directory durch, das der Mandant verwendet.
- Wiederholen Sie die Schritte 9 und 10 für jeden einem Mandanten zugeordneten Identitätsanbieter.

Voraussetzungen

- [Erstellen eines Administrators für jeden hinzugefügten Mandanten](#).
- Überprüfen Sie, ob Sie über Zugriffsberechtigungen für das Active Directory verfügen.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Verzeichnisse** aus.
- 2 Klicken Sie auf das Symbol **Verzeichnis hinzufügen (+)** und wählen Sie **Active Directory über LDAP/IWA hinzufügen** aus.
- 3 Geben Sie Ihre Active Directory-Kontoeinstellungen ein.
 - ◆ Für nicht-native Active Directories

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie Active Directory über LDAP aus, wenn ein nicht-natives Active Directory verwendet wird.
Dieses Verzeichnis unterstützt den DNS-Dienstspeicherort	Deaktivieren Sie diese Option.
Basis-DN	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: cn=users,dc=rainpole,dc=local .

Option	Beispieleingabe
Bind-DN	Geben Sie den vollständigen definierten Namen (DN, Distinguished Name), einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Beispiel: cn=config_admin infra,cn=users,dc=rainpole,dc=local .
Bind-DN-Kennwort	Geben Sie das Active Directory-Kennwort für das Konto ein, das nach Benutzern suchen kann, und klicken Sie auf Testverbindung , um die Verbindung zum konfigurierten Verzeichnis zu testen.

◆ Für native Active Directories

Option	Beispieleingabe
Verzeichnisname	Geben Sie einen eindeutigen Verzeichnisnamen ein. Wählen Sie Active Directory (Integrierte Windows-Authentifizierung) aus, wenn „Natives Active Directory“ verwendet wird.
Domänenname	Geben Sie den Namen der Domäne ein, der beigetreten werden soll.
Benutzername des Domänenadministrators	Geben Sie den Benutzernamen für den Domänenadministrator ein.
Kennwort des Domänenadministrators	Geben Sie das Kennwort für das Konto des Domänenadministrators ein.
Bind-Benutzer-UPN	Geben Sie als Benutzernamen die E-Mail-Adresse des Benutzers ein, der die Domäne authentifizieren kann.
Bind-DN-Kennwort	Geben Sie das Kennwort des Active Directory-Bind-Kontos für das Konto ein, das nach Benutzern suchen kann.

4 Klicken Sie auf **Speichern und weiter**.

Auf der Seite **Domänen auswählen** wird die Liste der Domänen angezeigt.

5 Übernehmen Sie die Einstellung für die Standarddomäne und klicken Sie auf **Weiter**.

6 Überprüfen Sie, ob die Attributnamen den richtigen Active Directory-Attributen zugeordnet sind, und klicken Sie auf **Weiter**.

7 Wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen.

a Klicken Sie auf das Symbol **Neu +**.

b Geben Sie die Benutzerdomäne ein und klicken Sie auf **Gruppen suchen**.

Geben Sie beispielsweise **dc=vcac,dc=local** ein.

c Um die Gruppen zur Synchronisierung zu wählen, klicken Sie auf **Auswählen** und **Weiter**.

d Wählen Sie auf der Seite **Benutzer auswählen** die Benutzer aus, die synchronisiert werden sollen, und klicken Sie auf **Weiter**.

Fügen Sie nur Benutzer und Gruppen hinzu, die vRealize Automation verwenden müssen. Wählen Sie **Geschachtelte Gruppen synchronisieren** nicht aus, es sei denn, alle Gruppen in der geschachtelten Gruppe müssen vRealize Automation verwenden.

- 8 Überprüfen Sie die Benutzer und Gruppen, die mit dem Verzeichnis synchronisiert werden, und klicken Sie auf **Verzeichnis synchronisieren**.

Für die Verzeichnissynchronisierung wird einige Zeit benötigt. Der Prozess wird im Hintergrund ausgeführt.

- 9 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus und klicken Sie auf Ihren neuen Identitätsanbieter.

Beispiel: **WorkspaceIDP__1**.

- 10 Fügen Sie auf der Seite des von Ihnen ausgewählten Identitätsanbieters jedem Knoten einen Connector hinzu.

- a Folgen Sie den Anweisungen unter **Hinzufügen eines Connectors**.
- b Aktualisieren Sie den Wert für die Eigenschaft **IdP-Hostname**, um auf den vollqualifizierten Domainennamen (FQDN) für den vRealize Automation-Lastausgleichsdienst zu verweisen.
- c Klicken Sie auf **Speichern**.

Nächste Schritte

[Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation-Quellumgebung.](#)

Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation -Quellumgebung

Vor der Migration müssen Sie eine Datenerfassung für die NSX-Netzwerk- und Sicherheitsbestandsliste in der vRealize Automation-Quellumgebung durchführen.

Diese Datenerfassung ist erforderlich, damit die Neukonfiguration des Lastausgleichsdiensts in vRealize Automation 7.4 möglich ist, wenn Sie von 7.1-, 7.2- oder 7.3-Bereitstellungen aus migrieren.

Hinweis Sie müssen diese Datenerfassung in Ihrer Quellumgebung nicht ausführen, wenn Sie eine Migration von vRealize Automation 6.2.x durchführen. vRealize Automation 6.2.x unterstützt das Neukonfigurieren des Lastausgleichsdiensts nicht.

Verfahren

- ◆ Führen Sie eine Datenerfassung für die NSX-Netzwerk- und Sicherheitsbestandsliste in Ihrer vRealize Automation-Quellumgebung durch, bevor Sie auf vRealize Automation 7.4 migrieren. Weitere Informationen finden Sie unter [Manuelles Starten der Endpoint-Datenerfassung](#) in *Verwalten von vRealize Automation*.

Nächste Schritte

[Manuelles Klonen der quellseitigen vRealize Automation IaaS Microsoft SQL-Datenbank.](#)

Manuelles Klonen der quellseitigen vRealize Automation IaaS Microsoft SQL-Datenbank

Vor der Migration müssen Sie eine Sicherungskopie Ihrer IaaS-Microsoft SQL-Datenbank in der vRealize Automation-Quellumgebung erstellen und diese in einer neuen leeren Datenbank wiederherstellen, die Sie in der vRealize Automation-Zielumgebung erstellt haben.

Voraussetzungen

- [Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation-Quellumgebung.](#)
- Suchen Sie nach Informationen zum Sichern und Wiederherstellen einer SQL Server-Datenbank. Suchen Sie nach Artikeln im [Microsoft Developer Network](#) zur Erstellung von kompletten SQL Server-Datenbanksicherungen und zur Wiederherstellung einer SQL Server-Datenbank an einem neuen Speicherort.

Verfahren

- ◆ Erstellen Sie eine vollständige Sicherungskopie Ihrer vRealize Automation 6.2.x- oder 7.x-IaaS-Microsoft SQL-Quelldatenbank. Mithilfe der Sicherung können Sie die SQL-Datenbank in einer neuen leeren Datenbank wiederherstellen, die Sie in der Zielumgebung erstellt haben.

Nächste Schritte

[Erstellen eines Snapshots der vRealize Automation-Zielumgebung.](#)

Erstellen eines Snapshots der vRealize Automation -Zielumgebung

Erstellen Sie einen Snapshot für jede virtuelle vRealize Automation-Zielmaschine. Wenn die Migration fehlgeschlagen ist, können Sie den Vorgang erneut unter Verwendung von Snapshots der virtuellen Maschine ausführen.

Weitere Informationen finden Sie in der vSphere-Dokumentation.

Voraussetzungen

[Manuelles Klonen der quellseitigen vRealize Automation IaaS Microsoft SQL-Datenbank.](#)

Nächste Schritte

Führen Sie einen der folgenden Vorgänge aus:

- [Migrieren von vRealize Automation-Quelldaten auf eine Minimalumgebung von vRealize Automation 7.4.](#)
- [Migrieren von vRealize Automation-Quelldaten in eine vRealize Automation 7.4-Hochverfügbarkeitsumgebung.](#)

Migrationsvorgänge

Die Art und Weise, wie Sie Ihre vRealize Automation-Quellumgebungsdaten migrieren, hängt davon ab, ob Sie in eine minimale Umgebung oder in eine Hochverfügbarkeitsumgebung migrieren.

Migrieren von vRealize Automation -Quelldaten auf eine Minimalumgebung von vRealize Automation 7.4

Sie können die Daten in Ihrer aktuellen vRealize Automation-Umgebung auf eine neue Installation von vRealize Automation 7.4 migrieren.

Alle Mandanten im Quellsystem müssen im Ziel erneut erstellt werden und das Verfahren „Identitätsquellen migrieren“ durchlaufen. Weitere Informationen finden Sie unter [Migrieren von Identitätsquellen auf VMware Identity Manager](#).

Voraussetzungen

- [Sammeln von für die Migration erforderlichen Informationen](#).
- [Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung](#).
- [Hinzufügen aller Mandanten aus der vRealize Automation-Quellumgebung zur Zielumgebung](#).
- [Erstellen eines Administrators für jeden hinzugefügten Mandanten](#).
- [Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration mit einer Minimalumgebung](#).
- [Manuelles Klonen der quellseitigen vRealize Automation IaaS Microsoft SQL-Datenbank](#).
- [Erstellen eines Snapshots der vRealize Automation-Zielumgebung](#).
- Melden Sie sich bei der Verwaltung der zieleseitigen vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der zieleseitigen vRealize Automation-Appliance eingegeben haben.

Verfahren

- 1 Wählen Sie **vRA-Einstellungen > Migration** aus.
- 2 Geben Sie die Informationen für die quellseitige vRealize Automation-Appliance ein.

Option	Beschreibung
Hostname	Der Hostname für die quellseitige vRealize Automation-Appliance.
Root-Benutzername	root
Root-Kennwort	Das bei der Bereitstellung der vRealize Automation-Appliance eingegebene Root-Kennwort.
Speicherort des Migrationspakets	Pfad zu einem vorhandenen Verzeichnis auf der Quell-Appliance von vRealize Automation 6.2.x oder 7.x, auf der das Migrationspaket erstellt wird.

- 3 Geben Sie die Informationen für die zieleseitige vRealize Automation-Appliance ein.

Option	Beschreibung
Root-Benutzername	root
Root-Kennwort	Das bei der Bereitstellung der zieleseitigen vRealize Automation-Appliance eingegebene Root-Kennwort.
Standardmandant	vsphere.local Sie können dieses Feld nicht ändern.

Option	Beschreibung
Administratorbenutzername	Administrator Sie können dieses Feld nicht ändern.
Administratorkennwort	Kennwort des Benutzers administrator@vsphere.local, das Sie bei der Bereitstellung der vRealize Automation-Zielumgebung eingegeben haben.

4 Geben Sie die Informationen für den zielseitigen IaaS-Datenbankserver ein.

Option	Beschreibung
Datenbankserver	Speicherort der Microsoft SQL Server-Instanz, in der sich die wiederhergestellte IaaS-Microsoft SQL-Datenbank von vRealize Automation befindet. Wenn eine benannte Instanz und ein nicht standardmäßiger Port verwendet werden, verwenden Sie das Format <i>SERVER,PORT\INSTANZ-NAME</i> . Wenn Sie den Ziel-Microsoft SQL Server so konfigurieren, dass er die AAG-Funktion (AlwaysOn Availability Group) verwendet, muss der Ziel-SQL-Server als AAG-Listenname ohne einen Port oder einen Instanznamen eingegeben werden.
Geklonter Datenbankname	Name der quellseitigen IaaS Microsoft SQL-Datenbank von vRealize Automation 6.2.x oder 7.x, die Sie auf dem Quellsystem gesichert und auf dem Zielsystem wiederhergestellt haben.
Authentifizierungsmodus	<ul style="list-style-type: none"> ■ Windows Bei Verwendung des Windows-Authentifizierungsmodus muss der Benutzer des IaaS-Diensts über die SQL Server-Rolle „db_owner“ verfügen. Dieselben Berechtigungen gelten bei Verwendung des SQL Server-Authentifizierungsmodus. ■ SQL Server SQL Server öffnet die Textfelder Anmeldename und Kennwort.
Anmeldename	Anmeldename des SQL Server-Benutzers mit der Rolle „db_owner“ für die geklonte IaaS Microsoft SQL-Datenbank.
Kennwort	Kennwort des SQL Server-Benutzers mit der Rolle „db_owner“ für die geklonte IaaS Microsoft SQL-Datenbank.
Ursprünglicher Verschlüsselungsschlüssel	Ursprünglicher Verschlüsselungsschlüssel, den Sie aus der Quellumgebung abrufen. Siehe Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung .
Neue Passphrase	Eine Reihe von Wörtern, die zur Generierung eines neuen Verschlüsselungsschlüssels verwendet werden. Sie verwenden diese Passphrase jedes Mal, wenn Sie eine neue IaaS-Komponente in der vRealize Automation-Zielumgebung installieren.

5 Klicken Sie auf **Validieren**.

Auf der Seite wird der Validierungsfortschritt angezeigt.

- Wenn alle Elemente erfolgreich validiert sind, fahren Sie mit Schritt 8 fort.
- Wenn ein Element nicht validiert wurde, prüfen Sie die Fehlermeldung und die Validierungsprotokolldatei auf den IaaS-Knoten. Informationen zu den Speicherorten der Protokolldateien finden Sie unter [Speicherorte des Migrationsprotokolls](#). Klicken Sie auf **Einstellungen bearbeiten** und bearbeiten Sie das entsprechende Element. Fahren Sie mit Schritt 7 fort.

6 Klicken Sie auf **Migrieren**.

Auf der Seite wird der Migrationsfortschritt angezeigt.

- Wenn die Migration erfolgreich ist, zeigt die Seite alle Migrationsaufgaben als abgeschlossen an.
- Wenn die Migration fehlgeschlagen ist, überprüfen Sie die Migrationsprotokolldateien auf der virtuellen Appliance und den IaaS-Knoten. Informationen zu den Speicherorten der Protokolldateien finden Sie unter [Speicherorte des Migrationsprotokolls](#).

Schließen Sie diese Schritte ab, bevor Sie die Migration erneut starten.

- a Setzen Sie die vRealize Automation-Zielumgebung auf den Stand zurück, von dem Sie vor der Migration einen Snapshot erstellt haben.
- b Stellen Sie die Ziel-IaaS-Microsoft SQL-Datenbank mithilfe der Sicherung der Quell-IaaS-Datenbank wiederher.

Nächste Schritte

[Aufgaben nach der Migration](#).

Migrieren von vRealize Automation -Quelldaten in eine vRealize Automation 7.4-Hochverfügbarkeitsumgebung

Sie können Ihre aktuellen vRealize Automation-Umgebungsdaten in eine neue Installation von vRealize Automation 7.4 migrieren, die als Hochverfügbarkeitsumgebung konfiguriert ist.

Alle Mandanten im Quellsystem müssen im Ziel erneut erstellt werden und das Verfahren „Identitätsquellen migrieren“ durchlaufen. Weitere Informationen finden Sie unter [Migrieren von Identitätsquellen auf VMware Identity Manager](#).

Voraussetzungen

- [Sammeln von für die Migration erforderlichen Informationen](#).
- [Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung](#).
- [Hinzufügen aller Mandanten aus der vRealize Automation-Quellumgebung zur Zielumgebung](#).
- [Erstellen eines Administrators für jeden hinzugefügten Mandanten](#).
- [Synchronisieren von Benutzern und Gruppen für einen Active Directory-Link vor der Migration auf eine Hochverfügbarkeitsumgebung](#).
- [Manuelles Klonen der quellseitigen vRealize Automation IaaS Microsoft SQL-Datenbank](#).
- [Erstellen eines Snapshots der vRealize Automation-Zielumgebung](#).
- Melden Sie sich bei der Verwaltung der zielseitigen vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der zielseitigen vRealize Automation-Appliance eingegeben haben.

Verfahren

- 1 Wählen Sie **vRA-Einstellungen > Migration** aus.

2 Geben Sie die Informationen für die quellseitige vRealize Automation-Appliance ein.

Option	Beschreibung
Hostname	Der Hostname für die quellseitige vRealize Automation-Appliance.
Root-Benutzername	root
Root-Kennwort	Das bei der Bereitstellung der quellseitigen vRealize Automation-Appliance eingegebene Root-Kennwort.

3 Geben Sie die Informationen für den Speicherort des Migrationspakets auf der vRealize Automation-Quell-Appliance ein.

Option	Beschreibung
Speicherort des Migrationspakets	Pfad zu einem vorhandenen Verzeichnis auf der Quell-Appliance von vRealize Automation 6.2.x oder 7.x, auf der das Migrationspaket erstellt wird.

4 Geben Sie die Informationen für die zielseitige vRealize Automation-Appliance ein.

Option	Beschreibung
Root-Benutzername	root
Root-Kennwort	Das bei der Bereitstellung der zielseitigen vRealize Automation-Appliance eingegebene Root-Kennwort.
Standardmandant	vsphere.local
Administratorbenutzername	Administrator
Administratorkennwort	Kennwort des Benutzers administrator@vsphere.local, das Sie bei der Bereitstellung der vRealize Automation-Zielumgebung eingegeben haben.

5 Geben Sie die Informationen für den zielseitigen IaaS-Datenbankserver ein.

Option	Beschreibung
Datenbankserver	Der Speicherort der Microsoft SQL Server-Instanz, in der sich die wiederhergestellte IaaS-Microsoft SQL-Datenbank von vRealize Automation befindet. Wenn eine benannte Instanz und ein nicht standardmäßiger Port verwendet werden, verwenden Sie das Format <code>SERVER,PORT\INSTANZ-NAME</code> . Wenn Sie den Ziel-Microsoft SQL Server so konfigurieren, dass er die AAG-Funktion (AlwaysOn Availability Group) verwendet, muss der Ziel-SQL-Server als AAG-Listenname ohne einen Port oder einen Instanznamen eingegeben werden.
Geklonter Datenbankname	Name der quellseitigen IaaS Microsoft SQL-Datenbank von vRealize Automation 6.2.x oder 7.x, die Sie auf dem Quellsystem gesichert und auf dem Zielsystem wiederhergestellt haben.
Authentifizierungsmodus	<ul style="list-style-type: none"> ■ Windows Bei Verwendung des Windows-Authentifizierungsmodus muss der Benutzer des IaaS-Diensts über die SQL Server-Rolle „db_owner“ verfügen. Dieselben Berechtigungen gelten bei Verwendung des SQL Server-Authentifizierungsmodus. ■ SQL Server SQL Server öffnet die Textfelder Anmeldename und Kennwort.

Option	Beschreibung
Anmeldename	Anmeldename des SQL Server-Benutzers mit der Rolle „db_owner“ für die geklonte IaaS Microsoft SQL-Datenbank.
Kennwort	Kennwort des SQL Server-Benutzers mit der Rolle „db_owner“ für die geklonte IaaS Microsoft SQL-Datenbank.
Ursprünglicher Verschlüsselungsschlüssel	Ursprünglicher Verschlüsselungsschlüssel, den Sie aus der Quellumgebung abrufen. Siehe Abrufen des Verschlüsselungsschlüssels aus der vRealize Automation-Quellumgebung .
Neue Passphrase	Eine Reihe von Wörtern, die zur Generierung eines neuen Verschlüsselungsschlüssels verwendet werden. Sie verwenden diese Passphrase jedes Mal, wenn Sie eine neue IaaS-Komponente in der vRealize Automation-Zielumgebung installieren.

6 Klicken Sie auf **Validieren**.

Auf der Seite wird der Validierungsfortschritt angezeigt.

- Wenn alle Elemente erfolgreich validiert sind, fahren Sie mit Schritt 8 fort.
- Wenn ein Element nicht validiert wurde, prüfen Sie die Fehlermeldung und die Validierungsprotokolldatei auf den IaaS-Knoten. Informationen zu den Speicherorten der Protokolldateien finden Sie unter [Speicherorte des Migrationsprotokolls](#). Klicken Sie auf **Einstellungen bearbeiten** und bearbeiten Sie das entsprechende Element. Fahren Sie mit Schritt 7 fort.

7 Klicken Sie auf **Migrieren**.

Auf der Seite wird der Migrationsfortschritt angezeigt.

- Wenn die Migration erfolgreich ist, zeigt die Seite alle Migrationsaufgaben als abgeschlossen an.
- Wenn die Migration fehlgeschlagen ist, überprüfen Sie die Migrationsprotokolldateien auf der virtuellen Appliance und den IaaS-Knoten. Informationen zu den Speicherorten der Protokolldateien finden Sie unter [Speicherorte des Migrationsprotokolls](#).

Schließen Sie diese Schritte ab, bevor Sie die Migration erneut starten.

- a Setzen Sie die vRealize Automation-Zielumgebung auf den Stand zurück, von dem Sie vor der Migration einen Snapshot erstellt haben.
- b Stellen Sie Ihre zweiseitige IaaS-Microsoft-SQL-Datenbank mithilfe der Sicherung der IaaS-Quelldatenbank wiederher.

Nächste Schritte

[Aufgaben nach der Migration](#).

Aufgaben nach der Migration

Nach der Migration von vRealize Automation führen Sie die Ihrer Situation entsprechenden Aufgaben nach der Migration aus.

Hinweis Nach der Migration der Identitätsquellen müssen Benutzer von vRealize Code Stream die vRealize Code Stream-Rollen manuell neu zuweisen.

Hinzufügen von Mandanten- und IaaS-Administratoren aus der vRealize Automation 6.2.x-Quellumgebung

Nach der Migration müssen Sie für jeden Mandanten die vRealize Automation 6.2.x-Mandantenadministratoren löschen und wiederherstellen.

Führen Sie für jeden Mandanten in der vRealize Automation-Zielkonsole das folgende Verfahren durch.

Hinweis Wenn Sie von einer vRealize Automation 7.x-Umgebung migrieren, müssen Sie dieses Verfahren nicht durchführen.

Voraussetzungen

- Erfolgreiche Migration auf die neueste Version von vRealize Automation.
- Melden Sie sich bei der zweiseitigen vRealize Automation-Konsole als **Administrator** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Ziel-Appliance eingegeben haben.

Verfahren

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf einen Mandantennamen.
- 3 Klicken Sie auf **Administratoren**.
- 4 Erstellen Sie eine Liste mit den Namen und Benutzernamen der einzelnen Mandantenadministratoren.
- 5 Löschen Sie sämtliche Administratoren, indem Sie der Reihe nach auf jeden Administrator zeigen und auf das Symbol „Löschen“ klicken.
- 6 Klicken Sie auf **Fertig stellen**.
- 7 Klicken Sie auf der Seite „Mandanten“ erneut auf den Namen des Mandanten.
- 8 Klicken Sie auf **Administratoren**.
- 9 Geben Sie die Namen aller gelöschten Benutzer in das entsprechende Suchfeld ein und drücken Sie die Eingabetaste.
- 10 Klicken Sie in den Suchergebnissen auf den Namen des jeweiligen Benutzers, um ihn wieder als Administrator hinzuzufügen.

Wenn Sie fertig sind, stimmen die Liste der Mandantenadministratoren und die Liste der gelöschten Administratoren überein.

- 11 Klicken Sie auf **Fertig stellen**.

Ausführen einer Testverbindung und Überprüfen von migrierten Endpoints

Bei einer Migration auf vRealize Automation 7.4 werden Änderungen an den Endpoints in der Zielumgebung vorgenommen.

Nach der Migration auf vRealize Automation 7.4 müssen Sie die Aktion **Testverbindung** für alle anwendbaren Endpoints durchführen. Außerdem müssen Sie möglicherweise einige migrierte Endpoints anpassen. Weitere Informationen finden Sie unter [Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints](#).

Die Standardsicherheitseinstellung für aktualisierte oder migrierte Endpoints ist, nicht vertrauenswürdige Zertifikate nicht zu akzeptieren.

Wenn Sie nicht vertrauenswürdige Zertifikate verwendet haben, müssen Sie nach dem Upgrade oder der Migration von einer früheren vRealize Automation-Installation die folgenden Schritte für alle vSphere- und NSX-Endpoints ausführen, um die Validierung des Zertifikats durchzuführen. Andernfalls schlagen die Endpoint-Vorgänge mit Zertifikatsfehlern fehl. Weitere Informationen finden Sie in den VMware Knowledgebase-Artikeln *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* unter <http://kb.vmware.com/kb/2150230> und *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* unter <http://kb.vmware.com/kb/2108294>.

- 1 Melden Sie sich nach dem Upgrade bzw. der Migration bei der vRealize Automation vSphere-Agent-Maschine an und starten Sie Ihre vSphere-Agents mithilfe der Registerkarte **Dienste** neu.
Im Fall einer Migration werden möglicherweise nicht alle Agents neu gestartet. Starten Sie diese bei Bedarf manuell neu.
- 2 Warten Sie, bis mindestens ein Ping-Bericht abgeschlossen ist. Es dauert eine oder zwei Minuten, bis ein Ping-Bericht abgeschlossen ist.
- 3 Wenn die vSphere-Agents die Datenerfassung gestartet haben, melden Sie sich bei vRealize Automation als IaaS-Administrator an.
- 4 Klicken Sie auf **Infrastruktur > Endpoints > Endpoints**.
- 5 Bearbeiten Sie einen vSphere-Endpoint und klicken Sie auf **Verbindung testen**.
- 6 Wenn eine Zertifikataufforderung angezeigt wird, klicken Sie auf **OK**, um das Zertifikat zu akzeptieren.
Wenn keine Zertifikataufforderung angezeigt wird, kann es sein, dass das Zertifikat derzeit korrekt in einer vertrauenswürdigen Rootzertifizierungsstelle der Windows-Maschine gespeichert ist, die Dienste für den Endpoint hostet, z. B. als Proxy-Agent-Maschine oder DEM-Maschine.
- 7 Klicken Sie auf **OK**, um die Zertifikatsannahme anzuwenden und den Endpoint zu speichern.
- 8 Wiederholen Sie diesen Vorgang für jeden vSphere-Endpoint.
- 9 Wiederholen Sie diesen Vorgang für jeden NSX-Endpoint.

Wenn die Aktion **Verbindung testen** erfolgreich war, aber einige Datenerfassungs- bzw. Bereitstellungsvorgänge fehlschlagen, können Sie dasselbe Zertifikat auf allen Agent-Maschinen installieren, die den Endpoint bedienen, sowie auf allen DEM-Maschinen. Alternativ dazu können Sie das Zertifikat von vorhandenen Maschinen deinstallieren und den oben genannten Vorgang für den fehlerhaften Endpoint wiederholen.

Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation 7.4-Umgebung

Nach der Migration müssen Sie in der vRealize Automation 7.4-Zielumgebung eine Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste durchführen.

Diese Datenerfassung ist erforderlich, damit die Neukonfiguration des Lastausgleichsdiensts in vRealize Automation 7.4 für 7.1-, 7.2- und 7.3-Bereitstellungen möglich ist.

Hinweis Sie müssen diese Datenerfassung nicht durchführen, wenn Sie eine Migration von vRealize Automation 6.2.x auf 7.4 durchgeführt haben.

Voraussetzungen

- [Durchführen einer Datenerfassung für das NSX-Netzwerk und die Sicherheitsbestandsliste in der vRealize Automation-Quellumgebung.](#)
- Führen Sie eine erfolgreiche Migration auf vRealize Automation 7.4 durch.

Verfahren

- ◆ Führen Sie eine Datenerfassung für die NSX-Netzwerk- und Sicherheitsbestandsliste in Ihrer vRealize Automation-Zielumgebung durch, bevor Sie auf vRealize Automation 7.4 migrieren. Weitere Informationen finden Sie unter [Manuelles Starten der Endpoint-Datenerfassung](#) in *Verwalten von vRealize Automation*.

Neukonfigurieren von Lastausgleichsdiensten nach der Migration auf eine Hochverfügbarkeitsumgebung

Wenn Sie auf eine Hochverfügbarkeitsumgebung migrieren, müssen Sie nach jeder abgeschlossenen Migration für jeden Lastausgleichsdienst die folgenden Aufgaben durchführen.

Voraussetzungen

[Migrieren von vRealize Automation-Quelldaten in eine vRealize Automation 7.4-Hochverfügbarkeitsumgebung.](#)

Verfahren

- 1 Stellen Sie die ursprünglichen Integritätsprüfungseinstellungen wieder her, damit Replikatknoten eingehenden Datenverkehr akzeptieren können, indem Sie die Lastausgleichsdienste für diese Elemente konfigurieren.
 - vRealize Automation-Appliance.
 - IaaS-Webserver, der den Model Manager hostet.
 - Manager Service.
- 2 Ändern Sie die Zeitüberschreitungseinstellungen für den Lastausgleichsdienst zurück auf den Standardwert.

Migrieren eines externen Orchestrator-Servers zu vRealize Automation 7.4

Sie können einen vorhandenen externen Orchestrator-Server in eine vRealize Orchestrator-Instanz migrieren, die in vRealize Automation eingebettet ist.

Sie können vRealize Orchestrator als externe Serverinstanz bereitstellen und vRealize Automation für die Verwendung mit dieser externen Instanz konfigurieren oder Sie können den vRealize Orchestrator-Server, der in der vRealize Automation-Appliance enthalten ist, konfigurieren und verwenden.

VMware empfiehlt, dass Sie Ihre externe vRealize Orchestrator-Instanz zu dem Orchestrator-Server migrieren, der in vRealize Automation integriert ist. Die Migration von einer externen zu einer eingebetteten Orchestrator-Instanz bietet folgende Vorteile:

- Reduzierung der Gesamtbetriebskosten
- Vereinfachung des Bereitstellungsmodells
- Verbesserung der betrieblichen Effizienz

Hinweis Ziehen Sie in Betracht, die externe vRealize Orchestrator-Instanz in den folgenden Fällen zu verwenden:

- Mehrere Mandanten in der vRealize Automation-Umgebung
- Geografisch verteilte Umgebung
- Bewältigung von Arbeitslasten
- Verwendung bestimmter-Plug-Ins wie z. B. Site Recovery Manager-Plug-In-Versionen vor Version 6.5.

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 6.0.3 Virtual Appliance	vRealize Automation 6.2.3	Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance auf vRealize Automation 7.4
vRealize Orchestrator 6.0.4 on Windows	vRealize Automation 6.2.4	Migrieren einer externen vRealize Orchestrator 6.x-Instanz unter Windows auf vRealize Automation 7.4
vRealize Orchestrator 6.0.4 Virtual Appliance	vRealize Automation 6.2.4	Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance auf vRealize Automation 7.4

vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 6.0.5 Virtual Appliance	vRealize Automation 6.2.5	Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance auf vRealize Automation 7.4
vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c	vRealize Automation 7.0 or IaaS	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database	vRealize Automation 7.0.1 or IaaS	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.1 Virtual Appliance	vRealize Automation 7.1	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.2 Virtual Appliance	vRealize Automation 7.2	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.3 Virtual Appliance	vRealize Automation 7.3	Migrieren einer externen Instanz von vRealize Orchestrator 7.x auf vRealize Automation 7.4
vRealize Orchestrator 6.0.3 on Windows	vRealize Automation 6.2.3	Migrieren der Orchestrator-Konfiguration von Windows auf eine virtuelle Appliance

Migrieren der Orchestrator-Konfiguration von Windows auf eine virtuelle Appliance

Sie können Ihre Windows-Standalone-Konfiguration von Orchestrator 5.5x und 6.x in die Orchestrator Appliance migrieren.

Voraussetzungen

- Stellen Sie einen Orchestrator-Knoten in der Zielversion bereit und konfigurieren Sie ihn. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen Orchestrator-Servers](#).
- Wenn der Quell-Orchestrator das SHA1-Paketsignaturzertifikat verwendet, stellen Sie sicher, dass Sie das Zertifikat mit einem stärkeren Signaturalgorithmus neu generieren. Der empfohlene Signaturalgorithmus lautet SHA2.
- Beenden Sie den Orchestrator-Serverdienst auf der quell- und zielseitigen Orchestrator-Instanz.
- Erstellen Sie eine Sicherungskopie der Datenbank des Orchestrator-Quellservers.

Hinweis Wenn Sie vorhaben, bis zur vollständigen Konfiguration der neuen Umgebung die Orchestrator-Quellumgebung zu verwenden, erstellen Sie eine Kopie der Quelldatenbank. Ist dies nicht der Fall, können Sie in der Konfiguration des Orchestrator-Ziels festlegen, dass es dieselbe Datenbank verwendet. Dies führt allerdings dazu, dass die Orchestrator-Quellumgebung nicht mehr funktionsfähig ist, da das Datenbankschema mit der Version des Orchestrator-Ziels aktualisiert wird.

Verfahren

- 1 Laden Sie das Migrationstool vom Orchestrator-Zielserver herunter.
 - a Melden Sie sich beim Control Center als **root** an.
 - b Öffnen Sie die Seite **Konfiguration exportieren/importieren** und klicken Sie auf die Registerkarte **Konfiguration importieren**.
 - c Laden Sie das Migrationstool wie in der Beschreibung auf der Seite angegeben oder direkt von https://Orchestrator-Server-IP_oder_DNS-Name:8283/vco-controlcenter/api/server/migration-tool herunter.

- 2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.

- a Extrahieren Sie das heruntergeladene Archiv im Orchestrator-Installationsordner.

Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows C:\Programme\VMware\Orchestrator.
- b Legen Sie die Umgebungsvariable PATH fest, wobei Sie den bin-Ordner der mit Orchestrator installierten Java-JRE wählen.
- c Navigieren Sie mithilfe der Windows-Befehlszeile zum Ordner bin im Installationsordner von Orchestrator.

Standardmäßig ist der Pfad zum Ordner bin C:\Programme\VMware\Orchestrator\migration-cli\bin.

- d Führen Sie den Befehl `export` über die Befehlszeile aus.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

Ein Archiv mit dem Dateinamen `orchestrator-config-export-Orchestrator-IP-Adresse_Datum_Uhrzeit.zip` wird in dem Ordner erstellt, in dem sich auch der Ordner `migration-cli` befindet.

- 3 Importieren Sie die Konfiguration in die Orchestrator-Zielinstanz.

- a Melden Sie sich beim Control Center als **root** an.
- b Öffnen Sie **Konfiguration exportieren/importieren** im Control Center und klicken Sie auf die Registerkarte **Konfiguration importieren**.
- c Navigieren Sie zur .ZIP-Datei, die aus der quellseitigen Orchestrator-Instanz importiert wurde, und wählen Sie sie aus.
- d Geben Sie das Kennwort ein, das Sie beim Exportieren der Konfiguration verwendet haben.

Lassen Sie das Feld leer, wenn Sie die Konfiguration ohne Kennwort exportiert haben.
- e Wählen Sie den Importtyp aus.

- f Wenn Sie die Konfiguration in einen externen Orchestrator-Server importieren, geben Sie an, ob die Datenbankeinstellungen importiert werden sollen.

Hinweis Wenn die Orchestrator-Quell- und Zielsever nicht so konfiguriert sind, dass sie dieselbe externe Datenbank verwenden, lassen Sie das Kontrollkästchen **Datenbankeinstellungen migrieren** leer, um eine Aktualisierung des Datenbankschemas auf die neuere Version zu verhindern. Andernfalls ist die Orchestrator-Quellumgebung nicht mehr funktionsfähig.

Sie müssen die Datenbank konfigurieren, die vom Orchestrator-Zielsever vor der Migration verwendet wird.

- g Klicken Sie auf **IMPORTIEREN**, um die Migration abzuschließen.

Eine Meldung, dass die Konfiguration erfolgreich importiert wurde, wird angezeigt. Der Orchestrator-Serverdienst der Orchestrator-Zielinstanz wird automatisch neu gestartet.

- 4 Wenn die Zielinstanz von vRealize Orchestrator einen anderen Authentifizierungsanbieterserver verwendet als die Orchestrator-Quelleinstanz, importieren Sie das SSL-Zertifikat des Authentifizierungsanbieters, dessen Verwendung konfiguriert ist, in den Trust Store der Orchestrator-Zielinstanz.
 - a Klicken Sie auf der Seite **Zertifikate** im Control Center auf **Aus URL importieren**.
 - b Geben Sie die URL der vRealize Automation- oder vSphere-Instanz an.

Eine Meldung bestätigt, dass die Migration erfolgreich abgeschlossen wurde. Der Orchestrator-Serverdienst wird automatisch neu gestartet.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Migrieren einer externen vRealize Orchestrator 6.x-Instanz unter Windows auf vRealize Automation 7.4

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.4 können Sie Ihre vorhandene externe Instanz von Orchestrator 6.x, die unter Windows installiert ist, zu dem Orchestrator-Server migrieren, der in vRealize Automation 7.4 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation-Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren oder migrieren Sie Ihre vRealize Automation-Instanz auf Version 7.4. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Automation* im Handbuch *Installieren oder Upgrade von vRealize Automation*.

- Wenn der Quell-Orchestrator das SHA1-Paketsignaturzertifikat verwendet, stellen Sie sicher, dass Sie das Zertifikat mit einem stärkeren Signaturalgorithmus neu generieren. Der empfohlene Signaturalgorithmus lautet SHA2.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Laden Sie das Migrationstool vom Orchestrator-Zielservers herunter.
 - a Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
 - b Laden Sie das Archiv `migration-tool.zip` herunter, das sich im Verzeichnis `/var/lib/vco/downloads` befindet.
- 2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.
 - a Legen Sie die Umgebungsvariable `PATH` fest, wobei Sie den `bin`-Ordner der mit Orchestrator installierten Java-JRE wählen.
 - b Laden Sie das Migrationstool auf dem Windows-Server hoch, auf dem der externe Orchestrator-Server installiert ist.
 - c Extrahieren Sie das heruntergeladene Archiv im Orchestrator-Installationsordner.
Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows `C:\Programme\VMware\Orchestrator`.
 - d Führen Sie die Windows-Befehlszeile als Administrator aus und navigieren Sie zum Ordner `bin` im Installationsordner von Orchestrator.
Standardmäßig ist der Pfad zum Ordner `bin` `C:\Programme\VMware\Orchestrator\migration-cli\bin`.
 - e Führen Sie den Befehl `export` über die Befehlszeile aus.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

Das Archiv wird im selben Ordner wie der Ordner `migration-cli` erstellt.

3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.4 integriert ist.

- a Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst auf der vRealize Automation-Appliance des integrierten vRealize Orchestrator-Servers.

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

- b Laden Sie die exportierte Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation-Appliance hoch.
- c Ändern Sie den Besitzer der exportierten Orchestrator-Konfigurationsdatei.

```
chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
```

- d Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
```

- e Entfernen Sie alle Zertifikate aus dem Keystore der Datenbank.

```
./vro-configuration.sh untrust --reset-db
```

4 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE if using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbankname
```

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

Damit haben Sie erfolgreich eine unter Windows installierte externe vRealize Orchestrator 6.x-Instanz zu einer vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.4 eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance auf vRealize Automation 7.4

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.4 können Sie Ihre vorhandene externe virtuelle Orchestrator 6.x-Appliance auf den Orchestrator-Server migrieren, der in vRealize Automation 7.4 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation-Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren oder migrieren Sie Ihre vRealize Automation-Instanz auf Version 7.4. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Automation* im Handbuch *Installieren oder Upgrade von vRealize Automation*.
- Wenn der Quell-Orchestrator das SHA1-Paketsignaturzertifikat verwendet, stellen Sie sicher, dass Sie das Zertifikat mit einem stärkeren Signaturalgorithmus neu generieren. Der empfohlene Signaturalgorithmus lautet SHA2.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Laden Sie das Migrationstool vom Orchestrator-Zielserver auf den Orchestrator-Quellserver.
 - a Melden Sie sich bei der virtuellen Appliance vRealize Orchestrator 6.x über SSH als **root** an.
 - b Führen Sie im Verzeichnis `/var/lib/vco` den Befehl `scp` aus, um das Archiv `migration-tool.zip` herunterzuladen.

```
scp root@vra-va-Hostname.Domäne.Name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Führen Sie den Befehl `unzip` zum Extrahieren des Archivs mit den Migrationstools aus.

```
unzip migration-tool.zip
```

- 2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.
 - a Führen Sie im Verzeichnis `/var/lib/vco/migration-cli/bin` den Befehl `export` aus.

```
./vro-migrate.sh export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

Im Ordner `/var/lib/vco` wird ein Archiv mit dem Dateinamen `orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip` erstellt.

- 3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.4 integriert ist.
 - a Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
 - b Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

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

- c Führen Sie im Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` den Befehl `scp` aus, um das exportierte Konfigurationsarchiv herunterzuladen.

```
scp root@Orchestrator-IP_oder_DNS-Name:/var/lib/vco/orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip ./
```

- d Ändern Sie den Besitzer der exportierten Orchestrator-Konfigurationsdatei.

```
chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
```

- e Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das vro-configure-Skript mit dem Befehl import ausführen.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-Orchestrator-Applic-  
ance-IP-Datum_Uhrzeit.zip
```

- 4 Wenn der externe Orchestrator-Server, von dem aus Sie migrieren möchten, die integrierte PostgreSQL-Datenbank verwendet, bearbeiten Sie deren Datenbankkonfigurationsdateien.

- a Heben Sie in der Datei /var/vmware/vpostgres/current/pgdata/postgresql.conf die Kommentierung der Zeile listen_addresses auf.

- b Legen Sie als Werte für listen_addresses Platzhalter (*) fest.

```
listen_addresses = '*'
```

- c Fügen Sie in der Datei /var/vmware/vpostgres/current/pgdata/pg_hba.conf eine Zeile an.

```
host all all vra-va-ip-address/32 md5
```

Hinweis Die Datei pg_hba.conf erfordert die Verwendung eines CIDR-Präfixformats anstelle einer IP-Adresse und Subnetzmaske.

- d Starten Sie den PostgreSQL-Serverdienst neu.

```
service vpostgres restart
```

- 5 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript vro-con-
figure mit dem Befehl db-migrate ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbe-  
nutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\; if using SQL authentication and MSSQL:  
jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE if using Windows au-  
thentication.
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbankname
```

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

- 6 Entfernen Sie alle Zertifikate aus dem Keystore der Datenbank.

```
./vro-configure.sh untrust --reset-db
```

- 7 Installieren Sie die Orchestrator-Plug-Ins erneut.
 - a Melden Sie sich beim Control Center als **root** an.
 - b Klicken Sie auf **Fehlerbehebung**.
 - c Klicken Sie auf **Plug-In-Neuinstallation erzwingen**.
- 8 Starten Sie den Orchestrator-Serverdienst.
- 9 Setzen Sie das System auf die Standardkonfiguration der Datei postgresql.conf und pg_hba.conf zurück.
 - a Starten Sie den PostgreSQL-Serverdienst neu.

Damit haben Sie erfolgreich eine externe virtuelle vRealize Orchestrator 6.x-Appliance auf eine vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.4 eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Migrieren einer externen Instanz von vRealize Orchestrator 7.x auf vRealize Automation 7.4

Sie können die Konfiguration aus Ihrer bestehenden externen Orchestrator-Instanz exportieren und sie in den in vRealize Automation integrierten Orchestrator-Server importieren.

Hinweis Wenn Sie mehrere vRealize Automation-Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren oder migrieren Sie Ihre vRealize Automation-Instanz auf Version 7.4. Weitere Informationen finden Sie unter *Aktualisieren von vRealize Automation* im Handbuch *Installieren oder Upgrade von vRealize Automation*.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Verfahren

- 1 Exportieren Sie die Konfiguration aus dem externen Orchestrator-Server.
 - a Melden Sie sich beim Control Center des externen Orchestrator-Servers als **root** oder als **Administrator** an (je nach Quellversion).
 - b Beenden Sie den Orchestrator-Serverdienst über die Seite **Startoptionen**, um unerwünschte Änderungen an der Datenbank zu vermeiden.
 - c Wechseln Sie zur Seite **Konfiguration exportieren/importieren**.
 - d Wählen Sie auf der Seite **Konfiguration exportieren** die Optionen **Serverkonfiguration exportieren**, **Paket-Plug-Ins** und **Plug-In-Konfigurationen exportieren**.
- 2 Migrieren Sie die exportierte Konfiguration in die eingebettete Orchestrator-Instanz.
 - a Laden Sie die exportierte Orchestrator-Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation-Appliance hoch.
 - b Melden Sie sich bei der vRealize Automation-Appliance über SSH als **root** an.
 - c Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

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

- d Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
```

3 Wenn der externe Orchestrator-Server, von dem aus Sie migrieren möchten, die integrierte PostgreSQL-Datenbank verwendet, bearbeiten Sie deren Datenbankkonfigurationsdateien.

- a Heben Sie in der Datei `/var/vmware/vpostgres/current/pgdata/postgresql.conf` die Kommentierung der Zeile `listen_addresses` auf.
- b Legen Sie als Werte für `listen_addresses` Platzhalter (*) fest.

```
listen_addresses = '*'
```

c Fügen Sie in der Datei `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` eine Zeile an.

```
host all all vra-va-ip-address/32 md5
```

Hinweis Die Datei `pg_hba.conf` erfordert die Verwendung eines CIDR-Präfixformats anstelle einer IP-Adresse und Subnetzmaske.

d Starten Sie den PostgreSQL-Serverdienst neu.

```
service vpostgres restart
```

4 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in einfache Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne\;useNTLMv2=TRUE if using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbankname
```

Die standardmäßigen Anmeldeinformationen für die Datenbank lauten:

<i>Datenbankname</i>	vmware
<i>Datenbankbenutzer</i>	vmware
<i>Kennwort_des_Datenbankbenutzers</i>	vmware

- 5 Entfernen Sie alle Zertifikate aus dem Keystore der Datenbank.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Installieren Sie die Orchestrator-Plug-Ins erneut.
 - a Melden Sie sich beim Control Center als **root** an.
 - b Klicken Sie auf **Fehlerbehebung**.
 - c Klicken Sie auf **Plug-In-Neuinstallation erzwingen**.
- 7 Starten Sie den Orchestrator-Serverdienst.
- 8 Setzen Sie das System auf die Standardkonfiguration der Datei `postgresql.conf` und `pg_hba.conf` zurück.
 - a Starten Sie den PostgreSQL-Serverdienst neu.

Damit haben Sie erfolgreich eine externe Orchestrator-Serverinstanz zu einer vRealize Orchestrator-Instanz migriert, die in vRealize Automation eingebettet ist.

Nächste Schritte

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe [Konfigurieren des integrierten vRealize Orchestrator-Servers](#).

Konfigurieren des integrierten vRealize Orchestrator -Servers

Nachdem Sie eine externe vRealize Orchestrator-Konfiguration exportiert und in vRealize Automation importiert haben, konfigurieren Sie den vRealize Orchestrator-Server, der in vRealize Automation integriert ist.

Voraussetzungen

Migrieren Sie die Konfiguration vom externen auf den internen vRealize Orchestrator-Server.

Verfahren

- 1 Melden Sie sich als Root-Benutzer bei einer Eingabeaufforderungssitzung auf der vRealize Automation-Appliance an.
- 2 Starten Sie die Dienste für das vRealize Orchestrator Control Center und den vRealize Orchestrator-Server:

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

- 3 Melden Sie sich als Root-Benutzer beim integrierten vRealize Orchestrator Control Center an.

<https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config>

Hinweis Wenn die externe und die interne Version von vRealize Orchestrator übereinstimmen, können Sie den nächsten Schritt überspringen.

- 4 Klicken Sie im Control Center auf **Konfiguration überprüfen** und vergewissern Sie sich, dass vRealize Orchestrator ordnungsgemäß konfiguriert ist.
- 5 Klicken Sie im Control Center auf **Zertifikate**, dann auf **Paketsignaturzertifikat** und generieren Sie ein neues Paketsignaturzertifikat.
- 6 Klicken Sie im Control Center auf **Anbieter für Authentifizierung konfigurieren**.
Standardmandant und **Administratorgruppe** sind auf die Standardwerte `vsphere.local` und `vsphere.local\vcoadmins` festgelegt. Ändern Sie die Standardwerte in die Werte für Ihre Umgebung.
- 7 Vergewissern Sie sich in der Verwaltungsschnittstelle der vRealize Automation-Appliance unter **Dienste**, dass `vco-server` REGISTRIERT ist.
- 8 Wählen Sie die vco-Dienste des externen vRealize Orchestrator-Servers aus und klicken Sie auf **Registrierung aufheben**.

Nächste Schritte

- Importieren Sie alle vertrauenswürdigen Zertifikate aus dem externen vRealize Orchestrator-Server in den Trust Store der integrierten vRealize Orchestrator-Instanz. Weitere Informationen finden Sie unter [Verwalten von Orchestrator-Zertifikaten](#).
- Fügen Sie die vRealize Automation-Replikatknoten zum vRealize Automation-Cluster hinzu, um die vRealize Orchestrator-Konfiguration zu synchronisieren.

Weitere Informationen finden Sie in der Beschreibung der *Neukonfiguration der eingebetteten Zielinstanz von vRealize Orchestrator zur Unterstützung der Hochverfügbarkeit* in *Installieren oder Upgrade von vRealize Automation*.

Hinweis Die vRealize Orchestrator-Instanzen werden automatisch zu Clustern zusammengefasst und stehen für die Verwendung zur Verfügung.

- Starten Sie den `vco-configurator`-Dienst auf allen Knoten im Cluster neu.
- Aktualisieren Sie den vRealize Orchestrator-Endpoint so, dass er auf den migrierten integrierten vRealize Orchestrator-Server verweist.
- Fügen Sie den vRealize Automation-Host und den IaaS-Host zur Bestandsliste des vRealize Automation-Plug-Ins hinzu, indem Sie die Workflows „Einen vRA-Host hinzufügen“ und „Den IaaS-Host eines vRA-Hosts hinzufügen“ ausführen.

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. Bei Verwendung einer externen vRealize Orchestrator-Instanz siehe hierzu [Aktualisierung eines externen vRealize Orchestrators zur Einstufung von vRealize Automation-Zertifikaten als vertrauenswürdig](#).

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/kb/2147612>.

Verfahren

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

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

- 2 Setzen Sie den 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
```

Control Center-Unterschiede zwischen externer und eingebetteter Orchestrator-Instanz

Einige Menüoptionen, die im Control Center einer externen vRealize Orchestrator-Instanz verfügbar sind, sind nicht in der Standardansicht des Control Center einer eingebetteten Orchestrator-Instanz enthalten.

Einige Optionen sind im Control Center des eingebetteten Orchestrator-Servers standardmäßig ausgeblendet.

Menüoption	Details
Lizenzierung	Die eingebettete Orchestrator-Instanz ist so vorkonfiguriert, dass vRealize Automation als Lizenzgeber verwendet wird.
Konfiguration exportieren/ importieren	Die Konfiguration der eingebetteten Orchestrator-Instanz ist in den exportierten vRealize Automation-Komponenten enthalten.
Datenbank konfigurieren	Die eingebettete Orchestrator-Instanz verwendet die Datenbank, die von vRealize Automation genutzt wird.
Programm zur Verbesserung der Kundenzufriedenheit	Über die Schnittstelle zur Verwaltung der vRealize Automation-Appliance können Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen. Lesen Sie die Informationen unter <i>Programm zur Verbesserung der Benutzerfreundlichkeit</i> im Handbuch <i>Verwalten von vRealize Automation</i> .

Andere nicht in der Standardansicht des Control Centers sichtbare Optionen sind das Textfeld **Hostadresse** und die Schaltfläche **REGISTRIERUNG AUFHEBEN** auf der Seite **Anbieter für Authentifizierung konfigurieren**.

Hinweis Wenn Sie sich über die vollständige Gruppe der Control Center-Optionen in vRealize Orchestrator, die in vRealize Automation integriert ist, informieren möchten, müssen Sie unter https://vra-va-Hostname.Domäne.Name_oder_Lastausgleichsadresse:8283/vco-controlcenter/#/?advanced die Seite für die erweiterte Verwaltung von Orchestrator aufrufen und diese mit der Funktionstaste F5 auf der Tastatur aktualisieren.

Neukonfiguration des vRealize Automation -Endpoints in der vRealize Orchestrator - Zielumgebung

Verwenden Sie das folgende Verfahren, um den vRealize Automation-Endpoint in der eingebetteten vRealize Orchestrator-Zielumgebung neu zu konfigurieren.

Voraussetzungen

- Erfolgreiche Migration auf die neueste Version von vRealize Automation.
- Stellen Sie mithilfe des vRealize Orchestrator-Client eine Verbindung zum zieleseitigen vRealize Orchestrator her. Informationen finden Sie unter [Verwenden des VMware vRealize Orchestrator-Client](#) in der *vRealize Orchestrator-Dokumentation*.

Verfahren

- 1 Wählen Sie aus dem oberen Dropdown-Menü **Design** aus.
- 2 Klicken Sie auf **Bestandsliste**.
- 3 Erweitern Sie **vRealize Automation**.

- Wenn Sie die Migration von einer Minimalumgebung durchgeführt haben, ermitteln Sie Endpoints, die den vollqualifizierten Domännennamen (FQDN) des Hosts der quellseitigen vRealize Automation-Appliance enthalten. Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, ermitteln Sie Endpoints, die den FQDN des Lastausgleichsdiensts der Quell-Appliance enthalten.

Wenn Sie Endpoints finden, die den FQDN enthalten, führen Sie die folgenden Schritte aus:	Wenn Sie keine Endpoints, die den FQDN enthalten, finden, führen Sie die folgenden Schritte aus:
<ol style="list-style-type: none"> Klicken Sie auf Workflows. Klicken Sie auf die Schaltfläche zum Erweitern und wählen Sie Bibliothek > vRealize Automation > Konfiguration aus. Führen Sie einen der folgenden Schritte aus: <ul style="list-style-type: none"> Wenn Sie die Migration von einer Minimalumgebung durchgeführt haben, führen Sie den Workflow Entfernen eines vRA-Hosts für jeden Endpoint, der den FQDN des Hosts der vRealize Automation-Quell-Appliance enthält, aus. Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, führen Sie den Workflow Entfernen eines vRA-Hosts für jeden Endpoint aus, der den FQDN des Lastausgleichsdiensts der Quell-Appliance enthält. 	<ol style="list-style-type: none"> Klicken Sie auf Ressourcen. Klicken Sie auf das Symbol zur Aktualisierung auf der oberen Symbolleiste. Klicken Sie auf die Erweiterungsschaltfläche und wählen Sie Bibliothek > vCACCAFE > Konfiguration aus. Führen Sie einen der folgenden Schritte aus: <ul style="list-style-type: none"> Wenn Sie die Migration von einer Minimalumgebung durchgeführt haben, löschen Sie jede Ressource, die eine URL-Eigenschaft mit dem FQDN des Hosts der vRealize Automation-Quell-Appliance aufweist. Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, löschen Sie jede Ressource, die eine URL-Eigenschaft mit dem Lastausgleichsdienst der vRealize Automation-Quell-Appliance enthält.

- Klicken Sie auf **Workflows**.
- Klicken Sie auf die Schaltfläche zum Erweitern und wählen Sie **Bibliothek > vRealize Automation > Konfiguration** aus.
- Um den zieleitigen vRealize Automation-Appliance-Host oder – wenn Sie eine Migration in eine Hochverfügbarkeitsbereitstellung durchgeführt haben – den Host mit Lastausgleich hinzuzufügen, führen Sie den Workflow **Hinzufügen eines vRA-Hosts mithilfe der Komponentenregistrierung** durch.

Neukonfiguration des vRealize Automation -Infrastruktur-Endpoints in den zieleitigen vRealize Orchestrator

Verwenden Sie das folgende Verfahren, um den vRealize Automation-Infrastruktur-Endpoint in dem zieleitig eingebetteten vRealize Orchestrator neu zu konfigurieren.

Voraussetzungen

- Erfolgreiche Migration auf die neueste Version von vRealize Automation.
- Stellen Sie mithilfe des vRealize Orchestrator-Client eine Verbindung zum zieleitigen vRealize Orchestrator her. Informationen finden Sie unter [Verwenden des VMware vRealize Orchestrator-Client](#) in der *vRealize Orchestrator-Dokumentation*.

Verfahren

- Wählen Sie aus dem oberen Dropdown-Menü **Design** aus.

- 2 Klicken Sie auf **Bestandsliste**.
- 3 Erweitern Sie **vRealize Automation Infrastructure**.
- 4 Wenn Sie die Migration aus einer Minimalumgebung durchgeführt haben, ermitteln Sie Endpoints, die den vollqualifizierten Domännennamen (FQDN) des quellseitigen vRealize Automation-Infrastrukturhosts enthalten. Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, ermitteln Sie Endpoints, die den FQDN des Lastausgleichsdiensts der Quell-Appliance enthalten.

Wenn Sie Endpoints finden, die den FQDN enthalten, führen Sie die folgenden Schritte aus:	Wenn Sie keine Endpoints finden, die den FQDN enthalten, führen Sie die folgenden Schritte aus:
<ol style="list-style-type: none"> 1 Klicken Sie auf Workflows. 2 Klicken Sie auf die Schaltfläche zum Erweitern und wählen Sie Bibliothek > vRealize Automation > Infrastrukturverwaltung > Konfiguration aus. 3 Führen Sie einen der folgenden Schritte aus: <ul style="list-style-type: none"> ■ Wenn Sie die Migration von einer Minimalumgebung durchgeführt haben, führen Sie den Workflow Entfernen eines IaaS-Hosts für jeden Endpoint aus, der den FQDN des quellseitigen vRealize Automation-Infrastrukturhosts enthält. ■ Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, führen Sie den Workflow Entfernen eines IaaS-Hosts für jeden Endpoint aus, der den FQDN des Lastausgleichsdiensts des quellseitigen vRealize Automation-Infrastrukturhosts enthält. 	<ol style="list-style-type: none"> 1 Klicken Sie auf Ressourcen. 2 Klicken Sie auf das Symbol zur Aktualisierung auf der oberen Symbolleiste. 3 Klicken Sie auf die Schaltfläche zum Erweitern und wählen Sie Bibliothek > vCAC > Konfiguration aus. 4 Führen Sie einen der folgenden Schritte aus: <ul style="list-style-type: none"> ■ Wenn Sie die Migration von einer Minimalumgebung durchgeführt haben, löschen Sie jede Ressource, die eine <code>host</code>-Eigenschaft mit dem FQDN des quellseitigen vRealize Automation-Infrastrukturhosts aufweist. ■ Wenn Sie die Migration von einer Hochverfügbarkeitsumgebung durchgeführt haben, löschen Sie jede Ressource, die eine <code>host</code>-Eigenschaft mit dem Lastausgleichsdienst des quellseitigen vRealize Automation-Infrastrukturhosts enthält.

- 5 Klicken Sie auf **Workflows**.
- 6 Klicken Sie auf die Schaltfläche zum Erweitern und wählen Sie **Bibliothek > vRealize Automation > Konfiguration** aus.
- 7 Führen Sie zum Hinzufügen des zieleitigen vRealize Automation-Infrastrukturhosts oder bei Migration zu einem Lastausgleichshost mit Hochverfügbarkeitsbereitstellung den Workflow **Hinzufügen des IaaS-Hosts eines vRA-Hosts** durch.

Installieren der vRealize Orchestrator -Anpassung

Sie können einen Workflow ausführen, um die angepassten Statusänderungsworkflow-Stubs und vRealize Orchestrator-Menüvorgangsworkflows zu installieren.

Weitere Informationen finden Sie unter [Installieren der vRealize Orchestrator-Anpassung](#).

Voraussetzungen

Erfolgreiche Migration auf die neueste Version von vRealize Automation.

Neukonfiguration eingebetteter vRealize Orchestrator -Infrastruktur-Endpoints in der vRealize Automation -Zielumgebung

Bei der Migration von einer vRealize Automation 6.2.x-Umgebung müssen Sie die URL des Infrastruktur-Endpoints aktualisieren, die auf den zieleitigen eingebetteten vRealize Orchestrator-Server verweist.

Voraussetzungen

- Führen Sie eine erfolgreiche Migration auf vRealize Automation 7.4 durch.
- Melden Sie sich an der zweiseitigen vRealize Automation-Konsole an.
 - a Öffnen Sie die vRealize Automation-Konsole unter Angabe des vollqualifizierten Domännennamens der zweiseitigen virtuellen Appliance: `https://vra-va-hostname.domain.name/vcac`.

Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domännennamens des Lastausgleichsdiensts der zweiseitigen virtuellen Appliance: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Melden Sie sich als IaaS-Administrator an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie auf der Seite „Endpoints“ den vRealize Orchestrator-Endpoint aus und klicken Sie auf **Bearbeiten**.
- 3 Bearbeiten Sie im Textfeld „Adresse“ die vRealize Orchestrator-Endpoint-URL.
 - Wenn Sie eine Migration in eine minimale Umgebung durchgeführt haben, ersetzen Sie die vRealize Orchestrator-Endpoint-URL durch `https://vra-va-hostname.domain.name:443/vco`.
 - Wenn Sie eine Migration in eine Hochverfügbarkeitsumgebung durchgeführt haben, ersetzen Sie die vRealize Orchestrator-Endpoint-URL durch `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Klicken Sie auf **OK**.
- 5 Führen Sie manuell eine Datenerfassung auf dem vRealize Orchestrator-Endpoint aus.
 - a Wählen Sie auf der Seite „Endpoints“ den vRealize Orchestrator-Endpoint aus.
 - b Wählen Sie **Aktionen > Datenerfassung** aus.

Stellen Sie sicher, dass die Datenerfassung erfolgreich verläuft.

Konfigurieren Sie den Azure-Endpoint in der vRealize Automation -Zielumgebung neu.

Nach der Migration müssen Sie den Microsoft Azure-Endpoint neu konfigurieren.

Führen Sie diesen Vorgang für jeden Azure-Endpoint durch.

Voraussetzungen

- Führen Sie eine erfolgreiche Migration auf die neueste Version von vRealize Automation 7.4 durch.
- Melden Sie sich an der zweiseitigen vRealize Automation-Konsole an.
 - a Öffnen Sie die vRealize Automation-Konsole unter Angabe des vollqualifizierten Domännennamens der zweiseitigen virtuellen Appliance: `https://vra-va-hostname.domain.name/vcac`.

Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domännennamens des Lastausgleichsdiensts der zweiseitigen virtuellen Appliance:
`https://vra-va-lb-hostname.domain.name/vcac.`

- b Melden Sie sich als IaaS-Administrator an.

Verfahren

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Wählen Sie einen Azure-Endpoint aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf **Details**.
- 5 Geben Sie in das Textfeld **Geheimer Clientschlüssel** den ursprünglichen geheimen Clientschlüssel ein.
- 6 Klicken Sie auf **Fertig stellen**.
- 7 Wiederholen Sie den Vorgang für jeden Azure-Endpoint.

Migrieren von vRealize Automation 6.2.x Automation Application Services auf 7.4

Sie können das VMware vRealize Application Services-Migrationstool verwenden, um Ihre vorhandenen Application Services-Blueprints und Bereitstellungsprofile von VMware vRealize Application Services 6.2.x auf vRealize Automation 7.4 zu migrieren.

Voraussetzungen

Erfolgreiche Migration auf die neueste Version von vRealize Automation.

Verfahren

- ◆ Führen Sie die folgenden Schritte durch, um das VMware vRealize Application Services-Migrationstool herunterzuladen.
 - a Klicken Sie auf [Download VMware vRealize Automation](#).
 - b Wählen Sie **Treiber & Tools > VMware vRealize Application Services-Migrationstool** aus.

Löschen der ursprünglichen vRealize Automation -IaaS-Microsoft SQL-Zieldatenbank

Sie können die ursprüngliche IaaS-Datenbank nach Abschluss der Migration löschen.

Voraussetzungen

Erfolgreiche Migration auf die neueste Version von vRealize Automation.

Ihre migrierte Umgebung verwendet nicht die ursprüngliche vRealize Automation-IaaS-Microsoft SQL-Datenbank, die Sie bei der Installation der vRealize Automation-Zielumgebung erstellt haben. Sie können diese ursprüngliche IaaS-Datenbank nach Abschluss der Migration unbesorgt vom Microsoft SQL Server löschen.

Aktualisieren der Menü-Inhalte für Datacenter-Standorte nach der Migration

Nach der Migration müssen Sie fehlende benutzerdefinierte Datacenter-Standorte im Dropdown-Menü **Standort** hinzufügen.

Nach der Migration auf die neueste Version von vRealize Automation werden die Standorte der Datacenter im Dropdown-Menü **Speicherort** auf der Seite „Computing-Ressourcen“ auf die Standardliste zurückgesetzt. Obwohl benutzerdefinierte Standorte der Datacenter fehlen, werden alle Computing-Ressourcenkonfigurationen erfolgreich migriert. Die `Vrm.DataCenter.Location`-Eigenschaft ist nicht betroffen. Sie können weiterhin benutzerdefinierte Datacenter-Standorte zum Menü **Standort** hinzufügen.

Voraussetzungen

Führen Sie eine Migration auf die neueste Version von vRealize Automation durch.

Verfahren

- ◆ Fügen Sie fehlende Datacenter-Standorte zum Dropdown-Menü **Standort** hinzu. Weitere Informationen finden Sie unter [Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen](#).

Upgrade von Software-Agents auf TLS 1.2

Nach der Migration von vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 auf 7.4 müssen Sie verschiedene Aufgaben durchführen, um die Software-Agents von Ihrer Quellumgebung auf Transport Layer Security (TLS) 1.2 zu aktualisieren.

Ab vRealize Automation 7.4 stellt TLS 1.2 das einzige unterstützte TLS-Protokoll für den Datenaustausch zwischen vRealize Automation und Ihrem Browser dar. Nach der Migration müssen Sie vorhandene VM-Vorlagen aus Ihrer vRealize Automation 7.1- oder 7.3-Quellumgebung und alle vorhandenen VMs aktualisieren.

Aktualisieren der VM-Vorlagen für die Quellumgebung

Nach Abschluss der Migration auf Version 7.4 müssen Sie vorhandene vRealize Automation 7.1-, 7.2-, 7.3- oder 7.3.1-Vorlagen aktualisieren, damit die Software-Agents das TLS 1.2-Protokoll verwenden.

Gast-Agent- und Agent-Bootstrap-Code muss in den Vorlagen für die Quellumgebung aktualisiert werden. Wenn Sie eine Option mit verknüpftem Klon verwenden, müssen Sie möglicherweise die Vorlagen mit den neu erstellten virtuellen Maschinen und deren Snapshots neu zuordnen.

Um Ihre Vorlagen zu aktualisieren, führen Sie die folgenden Aufgaben durch.

- 1 Melden Sie sich bei vSphere an.
- 2 Konvertieren Sie jede Vorlage aus vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 in eine virtuelle Maschine und schaltet Sie die Maschine ein.
- 3 Importieren Sie das entsprechende Software-Installationsprogramm und führen Sie es auf jeder virtuellen Maschine aus.
- 4 Konvertieren Sie jede virtuelle Maschine zurück in eine Vorlage.

Wenden Sie dieses Verfahren bei der Suche nach den Software-Installationsprogrammen für Linux oder Windows an.

Voraussetzungen

- [Anwenden des Software-Agent-Patches](#), wenn Sie eine Migration von vRealize Automation 7.1 oder 7.3 auf 7.4 durchgeführt haben.
- Erfolgreiche Migration von vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 auf 7.4.

Verfahren

- 1 Starten Sie einen Browser und öffnen Sie die Begrüßungsseite der vRealize Automation 7.4-Appliance mit dem vollqualifizierten Domännennamen für die virtuelle Appliance: `https://vra-va-hostname.domain.name`.
- 2 Klicken Sie auf die **Gast- und Software-Agent-Seite**.
- 3 Befolgen Sie die Anweisungen für die Installationsprogramme für Linux- oder Windows-Software.

Nächste Schritte

[Identifizieren von virtuellen Maschinen, für die ein Software-Agent-Upgrade erforderlich ist.](#)

Identifizieren von virtuellen Maschinen, für die ein Software-Agent-Upgrade erforderlich ist

Sie können den Integritätsdienst in der vRealize Automation-Konsole verwenden, um virtuelle Maschinen zu identifizieren, für die ein Software-Agent-Update auf TLS 1.2 erforderlich ist.

Manchmal aktualisiert der auf Ihre vRealize Automation-Quellumgebung angewendete Patch nicht alle virtuellen Maschinen. Sie können den Integritätsdienst verwenden, um die virtuellen Maschinen zu identifizieren, für die ein Software-Agent-Update auf TLS 1.2 erforderlich ist. Alle Software-Agents in der Zielumgebung müssen für Vorgänge nach erfolgter Bereitstellung aktualisiert werden.

Voraussetzungen

- [Anwenden des Software-Agent-Patches](#), wenn Sie eine Migration von vRealize Automation 7.1 oder 7.3 auf 7.4 durchgeführt haben.
- Sie haben vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 erfolgreich auf 7.4 migriert.
- Sie sind bei vRealize Automation 7.4 auf der primären virtuellen Appliance angemeldet.

Verfahren

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

Option	Kommentar
Name	Geben Sie Software-Agent-Überprüfung ein.
Beschreibung	Fügen Sie optional eine Beschreibung hinzu. Beispiel: Software-Agents für Upgrade auf TLS 1.2 suchen
Produkt	Wählen Sie vRealize Automation 7.4.0 aus.
Planen	Wählen Sie „Keine“ aus.

- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Testsuites auswählen“ die Optionen **Systemtests für vRealize Automation** und **Mandantentests für vRealize Automation** aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein.

Tabelle 1-84. Virtuelle vRealize Automation -Appliance

Option	Beschreibung
Adresse des öffentlichen Webservers	<ul style="list-style-type: none"> ■ Bei einer minimalen Bereitstellung ist dies die Basis-URL für den vRealize Automation-Appliance-Host. Beispielsweise <code>https://va-host.domain/</code>. ■ Bei einer High Availability-Bereitstellung ist dies die Basis-URL für den vRealize Automation-Lastausgleichsdienst. Beispiel: <code>https://load-balancer-host.domain/</code>.
Adresse der SSH-Konsole	Vollqualifizierter Domänenname der vRealize Automation-Appliance. Beispiel: <code>va-host.domain</code> .
Benutzer der SSH-Konsole	root
Kennwort der SSH-Konsole	Kennwort für Root.
Max. Antwortzeit für Dienst (ms)	Übernehmen Sie den Standardwert: 2000

Tabelle 1-85. vRealize Automation -Systemmandant

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

Tabelle 1-86. vRealize Automation -Festplattenspeicherüberwachung

Option	Beschreibung
Warnschwellenwert (in Prozent)	Übernehmen Sie den Standardwert: 75
Kritischer Schwellenwert (in Prozent)	Übernehmen Sie den Standardwert: 90

Tabelle 1-87. vRealize Automation -Mandant

Option	Beschreibung
Zu testender Mandant	Zu Testzwecken ausgewählter Mandant.
Benutzername des Fabric-Administrators	Benutzername des Fabric-Administrators. Beispiel: <code>admin@va-host.local</code> . Hinweis Dieser Fabric-Administrator muss auch über eine Mandantenadministrator- und eine IaaS-Administratorrolle verfügen, um alle Tests ausführen zu können.
Kennwort des Fabric-Administrators	Kennwort des Fabric-Administrators.

- 8 Klicken Sie auf **Weiter**.

- 9 Überprüfen Sie die Informationen auf der Seite „Übersicht“ und klicken Sie auf **Beenden**.
Die Konfiguration der Software-Agent-Überprüfung ist abgeschlossen.
- 10 Klicken Sie auf der Karte für die Software-Agent-Überprüfung auf **Ausführen**.
- 11 Wenn der Test abgeschlossen ist, klicken Sie auf die Mitte der Karte für die Software-Agent-Überprüfung.
- 12 Navigieren Sie auf der Ergebnisseite der Software-Agent-Überprüfung durch die Testergebnisse und suchen Sie den Test für die Software-Agent-Version in der Spalte „Name“. Wenn das Testergebnis „Fehlgeschlagen“ lautet, klicken Sie in der Spalte „Ursache“ auf den Link **Ursache**, um die virtuellen Maschinen mit veralteten Software-Agents anzuzeigen.

Nächste Schritte

Wenn Sie über virtuelle Maschinen mit einem veralteten Software-Agent verfügen, finden Sie weitere Informationen unter [Upgrade von Software-Agents auf vSphere](#).

Upgrade von Software-Agents auf vSphere

Nach der Migration können Sie beliebige veraltete Software-Agents auf vSphere auf TLS 1.2 aktualisieren. Verwenden Sie hierfür die Verwaltungsschnittstelle der vRealize Automation-Appliance.

Dieses Verfahren aktualisiert die veralteten Software-Agents auf den virtuellen Maschinen aus Ihrer Quellumgebung auf TLS 1.2 und ist für die Migration auf vRealize Automation 7.4 erforderlich.

Voraussetzungen

- [Anwenden des Software-Agent-Patches](#), wenn Sie eine Migration von vRealize Automation 7.1 oder 7.3 auf 7.4 durchgeführt haben.
- Erfolgreiche Migration von vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 auf 7.4.
- Sie haben den Integritätsdienst verwendet, um virtuelle Appliances mit veralteten Software-Agents zu identifizieren.

Verfahren

- 1 Melden Sie sich auf der primären vRealize Automation-Appliance bei der Verwaltungskonsolle der vRealize Automation-Appliance als **Root** mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance eingegeben haben.
Öffnen Sie in einer Hochverfügbarkeitsumgebung die Verwaltungsschnittstelle der Appliance auf der Master-Appliance.
- 2 Klicken Sie auf **vRA-Einstellungen > SW-Agents**.
- 3 Klicken Sie auf **TLS 1.0, 1.1 aktivieren und deaktivieren**.
Der Status von TLS v1.0, v1.1 lautet AKTIVIERT.

- 4 Geben Sie für die Mandantenanmeldedaten die angeforderte Informationen für die quellseitige vRealize Automation-Appliance ein.

Option	Beschreibung
Mandantenname	Name des Mandanten auf der quellseitigen vRealize Automation-Appliance. Hinweis Die Mandantenbenutzer muss über die zugewiesene Rolle „Softwarearchitekt“ verfügen.
Benutzername	Benutzername des Mandantenadministrators auf der quellseitigen vRealize Automation-Appliance.
Kennwort	Kennwort des Mandantenadministrators.

- 5 Klicken Sie auf **Testverbindung**.

Wenn eine Verbindung hergestellt werden konnte, wird eine Erfolgsmeldung angezeigt.

- 6 Geben Sie für die quellseitige Appliance die IP-Adresse oder den vollqualifizierten Domännennamen der quellseitigen vRealize Automation-Appliance ein.

Die quellseitige Appliance und die zielseitige Appliance müssen beide dieselben Mandantenanmeldedaten verwenden.

- 7 Klicken Sie auf **Batches auflisten**.

Die Tabelle „Batch-Auswahlliste“ wird angezeigt.

- 8 Klicken Sie auf **Anzeigen**.

Eine Tabelle mit einer Liste von virtuellen Maschinen mit veralteten Software-Agents wird angezeigt.

- 9 Aktualisieren Sie den Software-Agent für die virtuellen Maschinen, die sich im Zustand AKTUALISIERBAR befinden.

- Um den Software-Agent in einer einzelnen virtuellen Maschine zu aktualisieren, klicken Sie für eine Gruppe von virtuellen Maschinen auf **Anzeigen**, identifizieren Sie die virtuelle Maschine, die Sie aktualisieren möchten, und klicken Sie auf **Ausführen**, um das Upgrade zu starten.
- Um den Software-Agent für eine Gruppe von virtuellen Maschinen zu aktualisieren, identifizieren Sie die zu aktualisierende Gruppe und klicken Sie auf **Ausführen**, um das Upgrade zu starten.

Wenn Sie mehr als 200 virtuelle Maschinen aktualisieren möchten, können Sie die Geschwindigkeit des Batch-Upgrades durch Eingabe von Werten für diese Parameter steuern.

Option	Beschreibung
Batchgröße	Die für das Batch-Upgrade ausgewählte Anzahl der virtuellen Maschinen. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.
Warteschlangentiefe	Die Anzahl der parallelen Upgrades, die gleichzeitig ausgeführt werden können. Beispielsweise 20. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.

Option	Beschreibung
Batchfehler	Die Anzahl der REST-Fehler, die zur Verlangsamung des Batch-Upgrades führt. Beispiel: Wenn Sie das aktuelle Batch-Upgrade nach 5 Fehlern stoppen möchten, um die Stabilität des Upgrades zu verbessern, geben Sie „5“ in das Textfeld ein.
Batchausfälle	Die Anzahl der fehlgeschlagenen Software-Agent-Upgrades, die dazu führt, dass die Batchverarbeitung verlangsamt wird. Beispiel: Wenn Sie das aktuelle Batch-Upgrade nach 5 Fehlern stoppen möchten, um die Stabilität des Upgrades zu verbessern, geben Sie „5“ in das Textfeld ein.
Batchabruf	Wie oft der Upgradevorgang abgefragt wird, um den Status des Upgrades zu überprüfen. Sie können diese Anzahl anpassen, um die Geschwindigkeit des Upgrades anzupassen.

Wenn der Upgradevorgang zu langsam ist oder zu viele nicht erfolgreiche Upgrades erzeugt, können Sie diese Parameter anpassen, um die Upgradeleistung zu verbessern.

Hinweis Durch Klicken auf **Aktualisieren** wird die Liste der Batches gelöscht. Dieser Schritt wirkt sich nicht auf den Upgradevorgang aus. Zudem werden Informationen darüber aktualisiert, ob TLS 1.2 festgelegt ist oder nicht. Darüber hinaus wird beim Klicken auf **Aktualisieren** auch eine Integritätsprüfung der vRealize Automation-Dienste durchgeführt. Wenn Dienste nicht ausgeführt werden, zeigt das System eine Fehlermeldung an und alle anderen Aktionsschaltflächen werden deaktiviert.

10 Klicken Sie auf **TLS 1.0, 1.1 aktivieren und deaktivieren**.

Der Status von TLS v1.0, v1.1 lautet DEAKTIVIERT.

Upgrade von Software-Agents auf Amazon Web Service oder Azure

Sie können veraltete Software-Agents auf Amazon Web Service (AWS) oder Azure manuell aktualisieren.

- Sie müssen die in der Reservierung des migrierten vRealize Automation-Servers angegebenen Tunneleigenschaften aktualisieren.

Voraussetzungen

- [Anwenden des Software-Agent-Patches](#), wenn Sie eine Migration von vRealize Automation 7.1 oder 7.3 auf 7.4 durchgeführt haben.
- Erfolgreiche Migration von vRealize Automation 7.1, 7.2, 7.3 oder 7.3.1 auf 7.4.
- Ein Softwaretunnel ist vorhanden und die IP-Adresse der virtuellen Maschine im Tunnel ist bekannt.

Verfahren

- 1 Erstellen Sie eine Knotendatei für jeden Knoten, für den Sie ein Upgrade durchführen müssen.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <$DestinationVRA-Server> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

2 Erstellen Sie eine Plandatei, um den Software-Agent auf einer Linux- oder Windows-VM zu aktualisieren.

- Ändern Sie die Datei für die Migration von Parametern unter „/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}“ so, dass diese den Wert der privaten IP-Adresse entsprechend dem AWS- oder Azure-Endpoint enthält.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
```

- Verwenden Sie diesen Befehl für die Aktualisierung einer Linux-Maschine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --sour-
ce_cloud_provider azure
```

- Verwenden Sie diesen Befehl für die Aktualisierung einer Windows-Maschine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --sour-
ce_cloud_provider azure
```

- Mit diesem Befehl wird die Plandatei ausgeführt.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Verwenden Sie diesen Befehl, um den Software-Agent mit der Knotendatei aus Schritt 1 und der Plandatei aus Schritt 2 zu aktualisieren.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Als Alternative können Sie diesen Befehl verwenden, um über die Knotendatei nur jeweils einen Knoten auszuführen. Geben Sie hierfür einen Knotenindex an.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Wenn Sie diesen Vorgang ausführen, können Sie den Protokollen aus der virtuellen vRealize Automation-Appliance und der Hostmaschine folgen, um den Fortschritt des Server-Agent-Upgrades anzuzeigen.

Nach dem Upgrade importiert der Upgradevorgang ein Softwareaktualisierungsskript für Windows oder Linux auf die virtuelle vRealize Automation 7.4-Appliance. Sie können sich bei dem virtuellen vRealize Automation-Appliance-Host anmelden, um sicherzustellen, dass die Softwarekomponente erfolgreich importiert wurde. Nach dem Importieren der Komponente wird eine Softwareaktualisierung an den Event Broker Service (EBS) gesendet, um die Softwareaktualisierungsskripte an die identifizierten virtuellen Maschinen weiterzuleiten. Wenn das Upgrade abgeschlossen ist und die neuen Software-Agents betriebsbereit sind, werden sie durch das Senden einer Ping-Anforderung an die neue virtuelle vRealize Automation-Appliance gebunden.

Hinweis Nützliche Protokolldateien

- Catalina-Ausgabe für Quell-vRealize Automation: `/var/log/vcac/catalina.out`. In dieser Datei stellen Sie fest, dass die Upgrade-Anforderungen während der Agent-Migrationen vorgenommen wurden. Diese Aktivität ist mit der Ausführung einer Software-Bereitstellungsanforderung identisch.
- Catalina-Ausgabe für Ziel-vRealize Automation: `/var/log/vcac/catalina.out`. In dieser Datei werden die Ping-Anforderungen der migrierten virtuellen Maschinen mit den 7.4.0-SNAPSHOT-Versionsnummern angegeben. Sie können diese berechnen, indem Sie die EBS-Themennamen vergleichen, z. B. `sw-agent-UUID`.
- Agent-Aktualisierungsordner in der Protokolldatei für das Master-Upgrade der zieleitigen vRealize Automation-Maschine: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. Mit dieser Datei können Sie nachverfolgen, welcher Upgradevorgang derzeit ausgeführt wird.

- Einzelne in Mandantenordnern verfügbare Protokolle: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Einzelne Knoten werden hier als LOT-Dateien mit Fehlern und laufenden Erweiterungen angezeigt.
- Migrierte VMs: `/opt/vmware-appdirector/agent/logs/darwin*.log`. Sie können diesen Speicherort, der die empfangenen Software-Aktualisierungsanforderungen sowie einen eventuellen Neustart des Agent-Bootstrap und Software-Agent auflistet, stichprobenhaft überprüfen.

Einstellung für Eigenschaftswörterbuch nach der Migration ändern

Legen Sie die Steuerelementeigenschaften für das Eigenschaftswörterbuch `Label` in Ihren Blueprints nach der Migration von vRealize Automation 6.2.x als nicht überschreibbar fest.

Das Steuerelement „Beschriftung“ im Eigenschaftswörterbuch von vRealize Automation 6.2.x ist in vRealize Automation 7.x nicht vorhanden. Während der Migration wird das Steuerelement `Label` im migrierten Eigenschaftswörterbuch in ein Steuerelement vom Typ `TextBox` übersetzt.

Legen Sie die betroffenen Eigenschaften nach der Migration als nicht überschreibbar fest. Dies können Sie entweder manuell im Eigenschaftswörterbuch von vRealize Automation vornehmen oder mithilfe der Export- und Importfunktionen.

Überprüfen der vRealize Automation 7.4-Zielumgebung

Sie können überprüfen, ob alle Daten erfolgreich zur vRealize Automation-Zielumgebung migriert wurden.

Voraussetzungen

- Führen Sie eine Migration auf die neueste Version von vRealize Automation durch.
- Melden Sie sich an der zieleseitigen vRealize Automation-Konsole an.
 - a Öffnen Sie die vRealize Automation-Konsole unter Angabe des vollqualifizierten Domännennamens der zieleseitigen virtuellen Appliance: `https://vra-va-hostname.domain.name/vcac`.
Öffnen Sie bei einer Umgebung mit Hochverfügbarkeit die Konsole unter Angabe des vollqualifizierten Domännennamens des Lastausgleichsdiensts der zieleseitigen virtuellen Appliance: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Melden Sie sich mit Ihrem Mandantenadministrator-Benutzernamen und Ihrem Kennwort an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verwaltete Maschinen** aus und stellen Sie sicher, dass alle verwalteten virtuellen Maschinen vorhanden sind.
- 2 Klicken Sie auf **Computing-Ressourcen**, wählen Sie jeden Endpoint aus und klicken Sie auf **Datenerfassung, Jetzt anfordern** und **Aktualisieren**, um sicherzustellen, dass die Endpoints funktionieren.
- 3 Klicken Sie auf **Design** und überprüfen Sie auf der Seite **Blueprints** die Elemente jedes Blueprints.
- 4 Klicken Sie auf **XaaS** und überprüfen Sie die Inhalte von **Benutzerdefinierte Ressourcen, Ressourcenzuordnungen, XaaS-Blueprints** und **Ressourcenaktionen**.

- 5 Wählen Sie **Administration > Katalogmanagement** aus und überprüfen Sie die Inhalte von **Dienste, Katalogelemente, Aktionen** und **Berechtigungen**.
- 6 Wählen Sie **Elemente > Bereitstellungen** aus und überprüfen Sie die Details für die bereitgestellten virtuellen Maschinen.
- 7 Wählen Sie auf der Seite „Bereitstellungen“ eine bereitgestellte, ausgeschaltete virtuelle Maschine aus, wählen Sie **Aktionen > Einschalten** aus und klicken Sie auf **Absenden** und **OK**. Überprüfen Sie, ob die virtuelle Maschine ordnungsgemäß eingeschaltet wird.
- 8 Klicken Sie auf **Katalog** und fordern Sie ein neues Katalogelement an.
- 9 Geben Sie auf der Registerkarte **Allgemein** die erforderlichen Informationen ein.
- 10 Klicken Sie auf das Symbol für die Maschine, übernehmen Sie alle Standardeinstellungen und klicken Sie auf **Absenden** und dann auf **OK**.
- 11 Stellen Sie sicher, dass die Anforderung erfolgreich abgeschlossen wird.

Fehlerbehebung bei Migrationen

Die Themen zur Fehlerbehebung bei Migrationen stellen Lösungen für Probleme bereit, die möglicherweise beim Migrieren von vRealize Automation entstehen.

PostgreSQL-Version verursacht Fehler

Eine vRealize Automation 6.2.x-Umgebung, in der eine aktualisierte PostgreSQL-Datenbank enthalten ist, blockiert den Administratorzugriff.

Problem

Wenn eine aktualisierte PostgreSQL-Datenbank von vRealize Automation 6.2.x verwendet wird, muss ein Administrator einen Eintrag zur Datei `pg_hba.conf` hinzufügen, die Zugriff auf diese Datenbank über vRealize Automation bereitstellt.

Lösung

- 1 Öffnen Sie die Datei `pg_hba.conf`.
- 2 Um Zugriff auf diese Datenbank zu gewähren, fügen Sie den folgenden Eintrag hinzu.

```
host all vcac-database-user vra-va-ip trust-method
```

Für einige virtuelle Maschinen wird während der Migration keine Bereitstellung erstellt

Virtuelle Maschinen, die zum Zeitpunkt der Migration den Status „Fehlt“ aufweisen, verfügen nicht über eine entsprechende in der Zielumgebung erstellte Bereitstellung.

Problem

Wenn eine virtuelle Maschine in der Quellumgebung während der Migration den Status „Fehlt“ aufweist, wird in der Zielumgebung keine entsprechende Bereitstellung erstellt.

Lösung

- ◆ Wenn eine virtuelle Maschine nach der Migration den Status „Fehlt“ verlässt, können Sie sie unter Verwendung der Massenimportfunktion in die Zielumgebung importieren.

Speicherorte des Migrationsprotokolls

Sie können Probleme bei der Validierung oder Migration möglicherweise beheben, indem Sie die Protokolle ansehen, in denen der Migrationsprozess aufgezeichnet wurde.

Tabelle 1-88. Quellseitige vRealize Automation -Appliance

Protokoll	Speicherort
Protokoll der Paketerstellung	/var/log/vmware/vcac/migration-package.log

Tabelle 1-89. Zielseitige vRealize Automation -Appliance

Protokoll	Speicherort
Protokoll der Migration	/var/log/vmware/vcac/migrate.log
Protokoll der Migrationsausführung	/var/log/vmware/vcac/mseq.migration.log
Ausgabeprotokoll der Migrationsausführung	/var/log/vmware/vcac/mseq.migration.out.log
Protokoll der Validierungsausführung	/var/log/vmware/vcac/mseq.validation.log
Ausgabeprotokoll der Validierungsausführung	/var/log/vmware/vcac/mseq.validation.out.log

Tabelle 1-90. Ziel- vRealize Automation -Infrastrukturknoten

Protokoll	Speicherort
Protokoll der Migration	C:\Programme (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log
Protokoll der Validierung	C:\Programme (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log

Katalogelemente werden nach der Migration im Servicekatalog aufgeführt, können aber nicht angefordert werden

Katalogelemente, die bestimmte Eigenschaftsdefinitionen aus früheren Versionen verwenden, werden im Servicekatalog zwar angezeigt, können aber nach der Migration auf die neueste Version von vRealize Automation nicht angefordert werden.

Problem

Wenn Sie eine Migration von 6.2.x oder einer früheren Version durchgeführt haben und Eigenschaftsdefinitionen mit diesen Steuerungstypen oder Attributen vorhanden waren, fehlen diese Elemente in den Eigenschaftsdefinitionen. Katalogelemente, die diese Definitionen verwenden, funktionieren nicht mehr auf dieselbe Weise wie vor der Durchführung der Migration.

- Steuerungstypen. Kontrollkästchen oder Verknüpfung.
- Attribute. Beziehung, reguläre Ausdrücke oder Eigenschaftslayouts.

Ursache

In vRealize Automation 7.0 und höher werden in Eigenschaftsdefinitionen diese Elemente nicht mehr verwendet. Sie müssen die Eigenschaftsdefinitionen neu erstellen oder sie neu konfigurieren, sodass eine vRealize Orchestrator-Skriptaktion anstelle der eingebetteten Steuerungstypen oder Attribute verwendet wird.

Migrieren Sie den Steuerungstyp oder die Attribute mithilfe einer Skriptaktion auf vRealize Automation 7.x.

Lösung

- 1 Erstellen Sie in vRealize Orchestrator eine Skriptaktion, die die Eigenschaftswerte zurückgibt. Die Aktion muss einen einfachen Typ zurückgeben, beispielsweise Zeichenfolgen, ganze Zahlen oder andere unterstützte Typen. In der Aktion können andere Eigenschaften, von denen sie abhängt, als Eingabeparameter angegeben werden.
- 2 Konfigurieren Sie die Produktdefinition in der vRealize Automation-Konsole.
 - a Wählen Sie **Administration > Eigenschaftenwörterbuch > Eigenschaftsdefinitionen** aus.
 - b Wählen Sie die Eigenschaftsdefinition aus und klicken Sie auf **Bearbeiten**.
 - c Wählen Sie aus dem Dropdown-Menü „Anzeigehinweis“ die Option **Dropdown** aus.
 - d Wählen Sie aus dem Dropdown-Menü „Werte“ die Option **Externe Werte** aus.
 - e Wählen Sie die Skriptaktion aus.
 - f Klicken Sie auf **OK**.
 - g Konfigurieren Sie die in der Skriptaktion enthaltenen Eingabeparameter. Um die bereits vorhandene Beziehung beizubehalten, binden Sie den Parameter an die andere Eigenschaft.
 - h Klicken Sie auf **OK**.

Optionsfelder für die Datenerfassung sind in vRealize Automation deaktiviert

Nach der Migration von vRealize Automation 6.2.x auf 7.x enthält die Seite „Computing-Ressourcen“ auf der Ziel-vRealize Automation deaktivierte Optionsfelder unter „Datenerfassung“.

Ursache

Wenn Sie einen Agent auf der Quellumgebung installieren, die auf einen Endpoint verweist, und einen Agent auf der Zielumgebung installieren, die auf denselben Endpoint verweist, der Agent jedoch einen anderen Namen hat, können Sie in der Zielumgebung als Administrator eine Testverbindung zu diesem Endpoint ausführen. Wenn Sie sich jedoch als Fabric-Administrator bei vRealize Automation auf der Zielumgebung anmelden, sind die Optionsfelder auf der Seite „Computing-Ressourcen“ unter „Datenerfassung“ deaktiviert.

Lösung

Vermeiden Sie diese Situation, indem Sie dem auf der Zielumgebung installierten Agent denselben Namen geben wie dem auf der Quellumgebung installierten Agent.

Fehlerbehebung bei Software-Agent-Upgrades

Wenn Sie die vRealize Automation-Verwaltungsschnittstelle für das Upgrade von Software-Agents verwenden, können Sie in den Protokolldateien die Ursache von möglicherweise auftretenden Problemen ermitteln.

Problem

Beim Upgrade von Software-Agents können Probleme auftreten. Wenn Sie die Protokolldateien während des Software-Agent-Upgrades überprüfen, können Sie möglicherweise auftretende Probleme ermitteln.

Hinweis Serverprotokolle

- Folgen Sie der `updateSoftwareAgents.log`-Datei auf dem Server, um den Vorgang zu beobachten: `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`.
- Folgen Sie der `catlaina.out`-Datei auf der Ziel-Appliance, um zu ermitteln, welche Software-Agents keine Fehler aufweisen: `/var/log/vcac/catalina.out`.

Suchen Sie nach einer Zeichenfolge wie „ping“ als Rückmeldung für 7.4.0-SNAPSHOT.

Sie können zusätzliche Informationen an folgenden Speicherorten finden.

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (pro Betriebssystem)

Bevor Sie ein umfassendes Batch-Upgrade vornehmen, sollten Sie immer erst ein Test-Upgrade der Software-Agents der virtuellen Appliance durchführen. Übersicht über den Vorgang:

- Schauen Sie sich die erste Anforderung an die virtuelle Ziel-Appliance genau an, um die Agent-Versionen zu ermitteln.
- Schauen Sie sich die Anforderung an die virtuelle Quell-Appliance für das Upgrade genau an.
- Schauen Sie sich die Agents genau an, die eine neue 7.4-Version in der virtuellen Ziel-Appliance melden.
- Beobachten Sie zwischen diesen Ereignissen die `updateSoftwareAgents.log`-Datei im `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`-Verzeichnis.

Hinweis Clientprotokolle

Linux-Agent-Protokolle sind im `appdirector`-Ordner für Agent-Protokolle gespeichert: `/opt/vmware-appdirector/agent/logs/*.log`

Möglicherweise werden Fehler ähnlich der folgenden angezeigt. Diese Fehler sind temporär, weil sich die EBS-Warteschlangen während des Upgrades verändern.

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] [] com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while polling events for subscription '{}'
```

org.springframework.web.client.HttpClientErrorException: 404 Not Found

at org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler\$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]