

Installieren von vRealize Automation

21. Juli 2021

vRealize Automation 7.5

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

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

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

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

Copyright © 2014-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

vRealize Automation-Installation	7
Aktualisierte Informationen	8
1 Überblick über die Installation	10
Informationen zur Installation	10
Neu in dieser Installation	11
Installationskomponenten	11
Die vRealize Automation-Appliance	11
Infrastructure as a Service	12
Bereitstellungstyp	15
Minimalbereitstellungen	15
Verteilte Bereitstellungen	16
Auswählen der Installationsmethode	19
2 Vorbereitung für die Installation	20
Allgemeine Vorbereitung	20
Konten und Kennwörter	21
Hostnamen und IP-Adressen	23
Latenz und Bandbreite	24
vRealize Automation-Appliance	25
vRealize Automation Appliance-Ports	25
IaaS-Windows-Server	28
Ports auf IaaS-Windows-Servern	29
IaaS-Webserver	31
IaaS-Manager Service-Host	32
IaaS SQL Server-Host	33
IaaS Distributed Execution Manager-Host	34
DEM-Worker mit Amazon Web Services	34
DEM-Workern mit Openstack oder PowerVC	34
DEM-Worker mit Red Hat Enterprise Virtualization	35
DEM-Worker mit SCVMM	36
Zertifikate	37
vRealize Automation-Zertifikatsanforderungen	38
Extrahieren von Zertifikaten und privaten Schlüsseln	39
3 Bereitstellen der vRealize Automation-Appliance	41
Informationen zur Bereitstellung der Appliance	41

Bereitstellen der vRealize Automation-Appliance	41
Hinzufügen von Netzwerkkarten vor Ausführung des Installationsprogramms	46
4 Installieren mit dem Installationsassistenten	49
Verwenden des Installationsassistenten für minimale Bereitstellungen	49
Starten des Installationsassistenten für eine Minimalbereitstellung	50
Installieren des Management-Agents	50
Abschließen des Installationsassistenten	52
Verwenden des Installationsassistenten für Unternehmensbereitstellungen	53
Starten des Installationsassistenten für eine Unternehmensbereitstellung	53
Installieren des Management-Agents	54
Abschließen des Installationsassistenten	56
5 Die Standard-Installationsschnittstellen	57
Verwenden der Standardschnittstellen für minimale Bereitstellungen	58
Checkliste für Minimalbereitstellung	58
Konfigurieren der vRealize Automation-Appliance	58
Installieren der IaaS-Komponenten	62
Verwenden der Standardschnittstellen für verteilte Bereitstellungen	70
Checkliste für die verteilte Bereitstellung	70
Deaktivieren der Integritätsprüfungen des Lastausgleichsdiensts	71
Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung	72
Konfigurieren der Webkomponente, des Manager Service und des vertrauenswürdigen DEM-Hostzertifikats	74
Arbeitsblätter zur Installation	75
Konfigurieren des Lastausgleichsdiensts	77
Konfigurieren von Appliances für vRealize Automation	78
Installieren der IaaS-Komponenten in einer verteilten Konfiguration	86
Installieren der Agents	118
Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned	119
Auswählen des Agent-Installationsszenarios	119
Installationsspeicherort und Anforderungen für Agents	120
Installieren und Konfigurieren des Proxy-Agents für vSphere	120
Installieren des Proxy-Agents für Hyper-V oder XenServer	127
Installieren des VDI-Agents für XenDesktop	132
Installieren des EPI-Agents für Citrix	136
Installieren des EPI-Agents für Visual Basic-Skripterstellung	140
Installieren des WMI-Agents für WMI-Remoteanforderungen	144
6 Automatische Installation	148
Informationen zur automatischen Installation	148
Ausführen einer automatischen Installation	149

Ausführen einer automatischen Installation des Management-Agents	150
Antwortdatei der unbeaufsichtigten Installation	151
Die Installationsbefehlszeile	152
Grundlagen für die Installation über die Befehlszeile	152
Befehlsnamen für die Installation	153
Die Installations-API	154
Konvertierung von Eigenschaften der automatischen Installation in JSON	155

7 Aufgaben nach der Installation 157

Zeitzone nicht ändern	157
Konfigurieren der FIPS-konformen Verschlüsselung	158
Aktivieren des automatischen Manager Service-Failovers	159
Informationen zum automatischen Manager Service-Failover	159
Automatisches Failover der PostgreSQL-Datenbank	160
Ersetzen von selbstsignierten Zertifikaten mit von einer Zertifizierungsstelle bereitgestellten Zertifikaten	161
Ändern von Hostnamen und IP-Adressen	161
Ändern des Hostnamens der Appliance	161
Ändern der IP-Adresse der Appliance	162
Anpassen der SQL-Datenbank für einen geänderten Hostnamen	164
Ändern der IP-Adresse eines IaaS-Servers	164
Ändern eines IaaS-Server-Hostnamens	166
Festlegen der Anmelde-URL auf einen benutzerdefinierten Namen	168
Entfernen eines Knotens der vRealize Automation-Appliance	169
Installieren des vRealize Log Insight-Agents	169
Ändern des VMware Remote Console-Proxy-Ports	169
Ändern eines Appliance-FQDN in ursprünglichen FQDN	170
Konfigurieren von SQL AlwaysOn Availability Group	171
Hinzufügen von Netzwerkkarten nach der Installation von vRealize Automation	171
Konfigurieren von statischen Routen	173
Zugriff auf Patch-Verwaltung	174
Konfigurieren des Zugriffs auf den Standardmandanten	175

8 Fehlerbehebung bei einer Installation 177

Standardspeicherorte für Protokolle	177
Rollback einer fehlgeschlagenen Installation wird ausgeführt	179
Rollback einer Minimalinstallation ausführen	179
Rollback einer verteilten Installation ausführen	180
Erstellen eines Support-Pakets	181
Allgemeine Fehlerbehebung bei der Installation	182
Installations- oder Aktualisierungsfehler mit einem Zeitüberschreitungsfehler des Lastausgleichsdiensts	182

Serverzeiten sind nicht synchronisiert	183
Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 werden möglicherweise leere Seiten angezeigt	183
Es kann kein Vertrauensverhältnis für den sicheren SSL/TLS-Kanal hergestellt werden	184
Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server	185
Konsolenschritte für die Erstkonfiguration von Inhalten	185
vRealize Automation-Lizenzen können nicht herabgestuft werden	186
Fehlerbehebung bei der vRealize Automation-Appliance	187
Installationsprogramme können nicht heruntergeladen werden	187
Falsche Berechtigungen für die Datei „Encryption.key“	188
Identity Manager der Verzeichnisverwaltung startet nach einem Neustart von horizon-workspace nicht	189
Falsche Zuweisungen von Appliance-Rollen nach Failover	190
Fehler nach dem Upgrade von Replikat- und Master-Knoten	191
Falsche Komponentendienstregistrierungen	192
Zusätzliche Netzwerkkarte (NIC) verursacht Fehler bei der Verwaltungsschnittstelle	194
Heraufstufen einer sekundären virtuellen Appliance zum Master ist nicht möglich	195
Der Aufbewahrungszeitraum des Active Directory-Synchronisierungsprotokolls ist zu kurz	195
RabbitMQ kann Hostnamen nicht auflösen	196
Fehlerbehebung bei IaaS-Komponenten	197
Distributed Transaction Coordinator-Verbindungen werden abgelehnt	197
Voraussetzungskorrektur kann keine .NET-Funktionen installieren	198
Überprüfen der Server-Zertifikate für IaaS	198
Fehler aufgrund der Anmeldedaten beim Ausführen des IaaS-Installers	199
Warnung wegen Speicherung der Einstellungen wird während IaaS-Installation angezeigt	200
Fehler beim Installieren des Website-Servers und der Distributed Execution Manager	200
IaaS-Authentifizierung schlägt während der Installation der IaaS-Web- und Modellverwaltung fehl	200
Model Manager-Daten und Webkomponenten können nicht installiert werden	201
IaaS-Windows-Server unterstützen kein FIPS	203
Interner Fehler durch Hinzufügen eines XaaS-Endpoints	203
Ein Proxy-Agent kann nicht deinstalliert werden	204
Fehler bei Maschinenanforderungen, wenn Remote-Transaktionen deaktiviert sind	204
Fehler bei der Kommunikation mit dem Manager Service	205
Geändertes Verhalten für die Anpassung von E-Mails	206
Fehlerbehebung bei Anmeldefehlern	207
Anmeldeversuche als IaaS-Administrator mit falsch formatierten UPN-Anmeldedaten schlagen ohne Begründung fehl	207
Anmeldung schlägt fehl bei Hochverfügbarkeit	208
Proxy verhindert VMware Identity Manager-Benutzeranmeldung	208

vRealize Automation-Installation

Dieser Leitfaden zur *Installation von vRealize Automation* enthält Anweisungen für die assistentengestützte, manuelle und automatische Installation von VMware vRealize™ Automation.

Hinweis Nicht alle Funktionen von vRealize Automation sind in allen Editionen verfügbar. Einen Vergleich des Funktionssatzes der verschiedenen Editionen finden Sie unter <https://www.vmware.com/products/vrealize-automation/>.

Zielgruppe

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datacenteroperationen vertraut sind.

Aktualisierte Informationen

In der folgenden Tabelle werden die Änderungen aufgelistet, die für diese Produktversion an *Installieren von vRealize Automation* vorgenommen wurden.

Revision	Beschreibung
XX TBD 202X	<ul style="list-style-type: none">■ Installieren des vRealize Automation-Management-Agents wurde aktualisiert.■ Aktivieren des automatischen Manager Service-Failovers wurde aktualisiert.■ Erstellen eines vRealize Automation-Support-Pakets wurde aktualisiert.■ Falsche vRealize Automation Komponentendienstregistrierungen wurde aktualisiert.
12. August 2020	Extrahieren von Zertifikaten und privaten Schlüsseln wurde aktualisiert.
14. FEB 2020	<ul style="list-style-type: none">■ IaaS-Windows-Server wurde aktualisiert.■ IaaS-Manager Service-Host wurde aktualisiert.■ IaaS SQL Server-Host wurde aktualisiert.■ Keine Änderung der vRealize Automation-Zeitzone wurde aktualisiert.■ Zugriff auf Patch-Verwaltung wurde aktualisiert.■ Distributed Transaction Coordinator-Verbindungen werden abgelehnt wurde hinzugefügt.■ Fehler bei Maschinenanforderungen, wenn Remote-Transaktionen deaktiviert sind wurde aktualisiert.
24. OKT 2019	Connector-Erinnerung wurde zu Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster hinzugefügt.
9. September 2019	Keine Änderung der vRealize Automation-Zeitzone wurde hinzugefügt.
14. Juni 2019	<ul style="list-style-type: none">■ Die Gruppenrichtlinieneinstellungen wurden in Konten und Kennwörter aktualisiert.■ Das englische Gebietsschema wurde in IaaS-Windows-Server aktualisiert.
30. Mai 2019	<ul style="list-style-type: none">■ Gruppenrichtlinieneinstellungen wurden in Konten und Kennwörter hinzugefügt.■ PowerShell 2 wurde entfernt und das englische Gebietsschema wurde in IaaS-Windows-Server hinzugefügt.
7. Mai 2019	Bei einigen Hyperlinks wurden Fehler behoben.
1. März 2019	Unter Informationen zur Installation von vRealize Automation wurden LCM-Links hinzugefügt.
12. Februar 2019	Die Java-Anforderung wurde auf Version 1.8 Update 181 oder höher aktualisiert.
13. November 2018	SQL Server 2017 wurde hinzugefügt.

Revision	Beschreibung
4. Oktober 2018	<ul style="list-style-type: none"> ■ Referenz zu erweiterter Hardware in IaaS SQL Server-Host hinzugefügt. ■ Timeout-Link zu Knowledgebase-Artikel in Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster hinzugefügt. ■ FQDN-Voraussetzung für Zertifikat zu Installieren zusätzlicher IaaS-Webserver-Komponenten und Installieren einer Manager Service-Backup-Komponente hinzugefügt. ■ In einen Knowledgebase-Artikel-Link in Entfernen eines Knotens der vRealize Automation-Appliance geändert. ■ Wichtiges Datenbankproblem in der Online-Hilfe eingefügt.
20. September 2018	Erste Produktversion.

Überblick über die vRealize Automation-Installation

1

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.

Dieses Kapitel enthält die folgenden Themen:

- [Informationen zur Installation von vRealize Automation](#)
- [Neu in dieser vRealize Automation-Installation](#)
- [vRealize Automation-Installationskomponenten](#)
- [Bereitstellungstyp](#)
- [Auswählen der Installationsmethode](#)

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 Lifecycle Manager installieren. Weitere Informationen finden Sie im Handbuch [vRealize Suite Lifecycle Manager Installation, Upgrade, and Management](#).

vRealize Suite Lifecycle Manager automatisiert die Installation, Konfiguration, das Upgrade, das Patchen, das Konfigurationsmanagement, die Drift-Standardisierung und den Systemzustand von einer zentralen Oberfläche aus. Klicken Sie hier, um [vRealize Suite Lifecycle Manager](#) zu installieren. Lifecycle Manager bietet IT-Managern für die Cloud-Verwaltung Ressourcen, um sich auf geschäftskritische Initiativen zu konzentrieren und gleichzeitig Wertschöpfung, Zuverlässigkeit und Konsistenz zu verbessern.

Neu in dieser vRealize Automation-Installation

Wenn Sie frühere Versionen von vRealize Automation installiert haben, beachten Sie die Änderungen im Installationsprozess für diese Version.

Die Verwaltungsschnittstelle der vRealize Automation-Appliance wurde geändert.

- Funktionen der Registerkarte „Datenbank“ wurden zur Registerkarte „Cluster“ verschoben. Die Registerkarte „Datenbank“ wurde entfernt, und die Registerkarte „Cluster“ wurde zu einer primären Registerkarte.
- Die Registerkarte „Migration“ wurde zu einer primären Registerkarte und umfasst jetzt die Migration von vRealize Automation und vRealize Orchestrator.
- Die Option „Support-Paket“ wurde zur Registerkarte „Protokolle“ verschoben.
- vRealize Code Stream wurde von der Registerkarte „Lizenzierung“ entfernt.

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 AutomationaaS 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-Webschnittstelle 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.

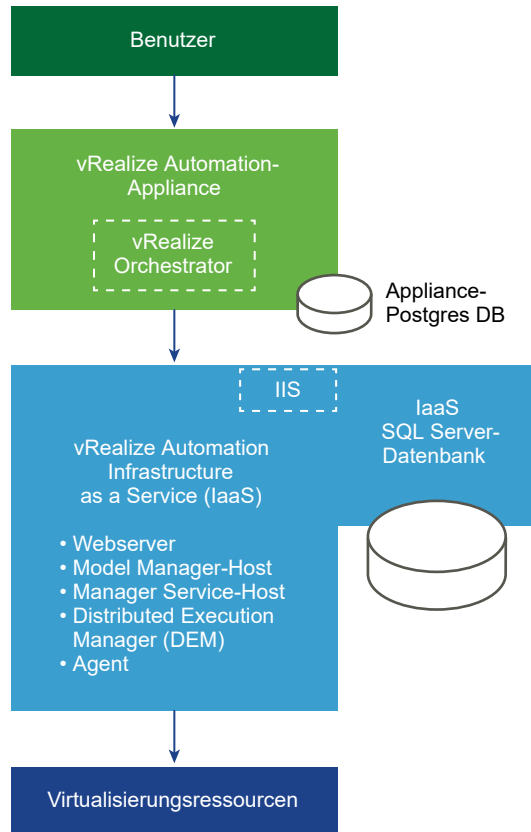
Bereitstellungstyp

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 1-1. Minimalbereitstellung von vRealize Automation

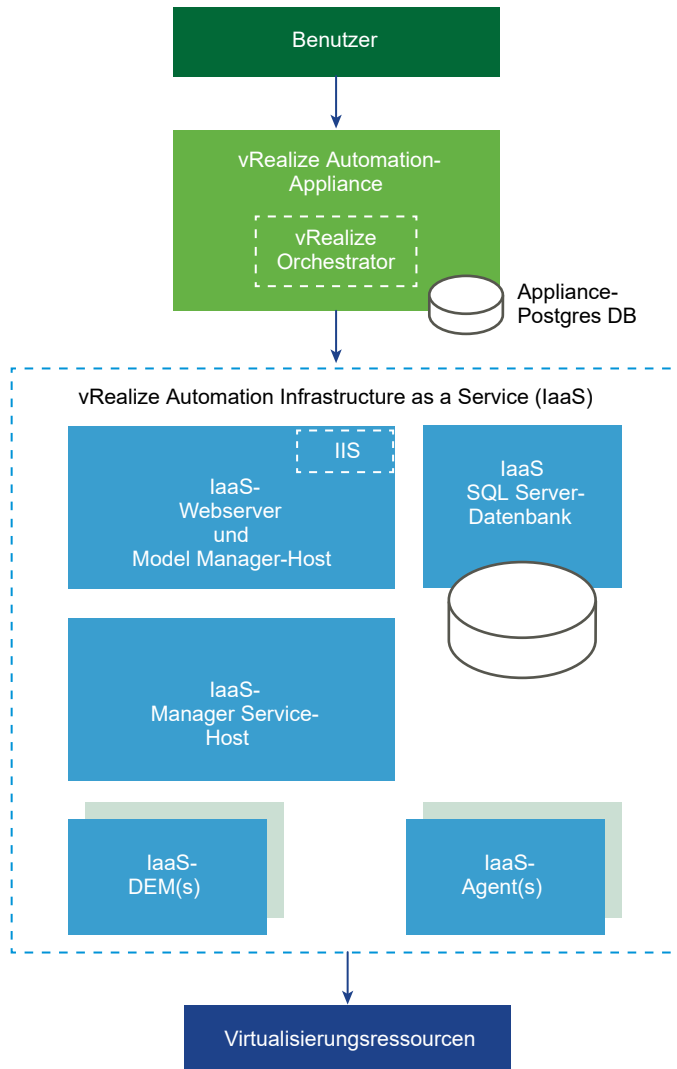


Eine Minimalbereitstellung kann nicht in eine Unternehmensbereitstellung konvertiert werden. Beginnen Sie zum Hochskalieren einer Bereitstellung mit einer kleinen Unternehmensbereitstellung und fügen Sie darin Komponenten hinzu. Eine Minimalbereitstellung wird als Ausgangspunkt nicht unterstützt.

Verteilte Bereitstellungen von vRealize Automation

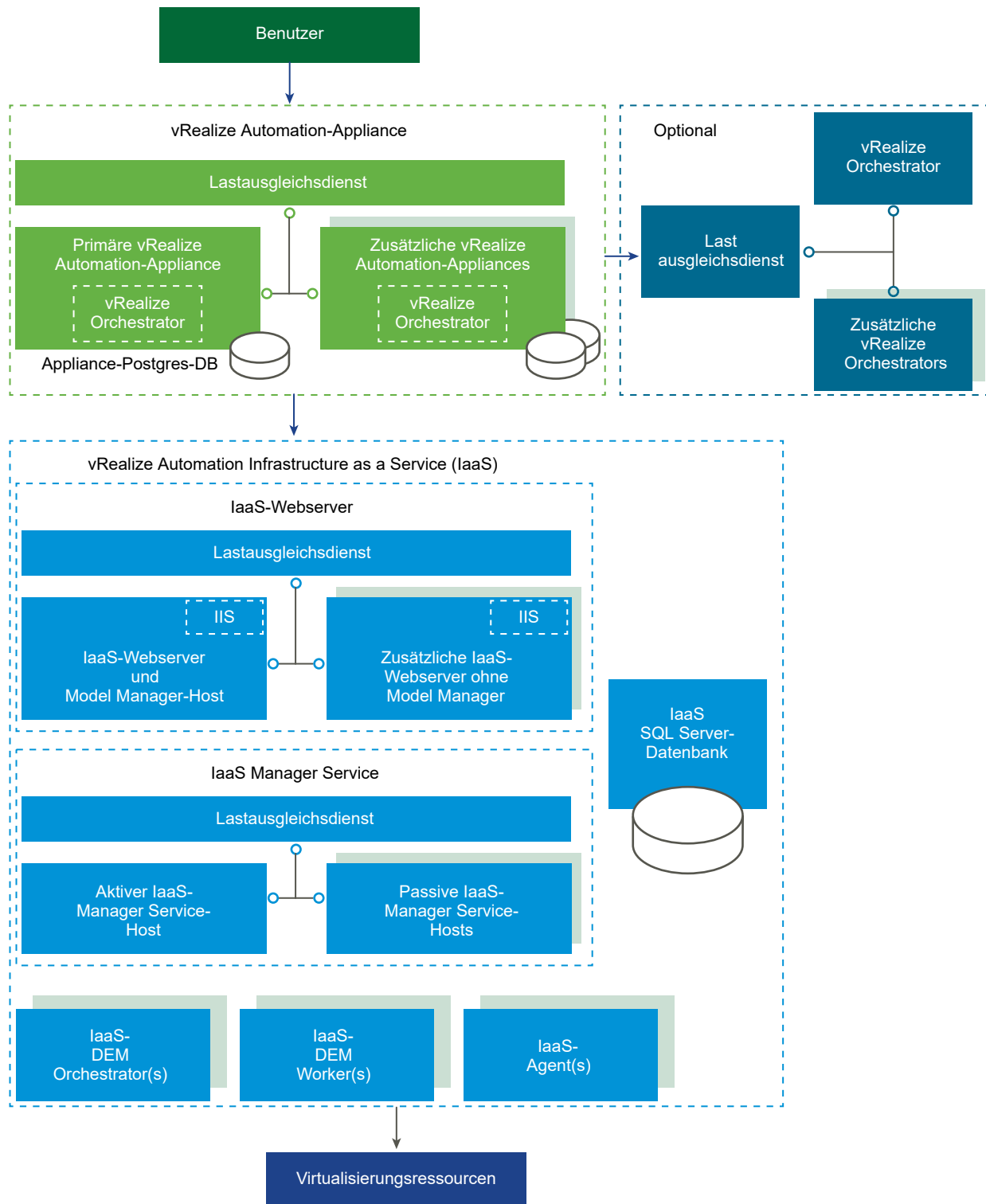
Verteilte Unternehmensbereitstellungen können verschiedene Größen haben. Eine einfache verteilte Bereitstellung kann vRealize Automation verbessern, indem IaaS-Komponenten auf separaten Windows-Servern gehostet werden (siehe folgende Abbildung).

Abbildung 1-2. 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 1-3. 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

2

Sie installieren vRealize Automation in einer vorhandenen Virtualisierungsinfrastruktur. Bevor Sie mit einer Installation beginnen, müssen Sie bestimmte umgebungsabhängige Anforderungen sowie Systemanforderungen erfüllen.

Dieses Kapitel enthält die folgenden Themen:

- [Allgemeine Vorbereitung](#)
- [Konten und Kennwörter](#)
- [Hostnamen und IP-Adressen](#)
- [Latenz und Bandbreite](#)
- [vRealize Automation-Appliance](#)
- [IaaS-Windows-Server](#)
- [IaaS-Webserver](#)
- [IaaS-Manager Service-Host](#)
- [IaaS SQL Server-Host](#)
- [IaaS Distributed Execution Manager-Host](#)
- [Zertifikate](#)

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.

- Wenn auf Ihrer Site Sicherheitseinstellungen für Gruppenrichtlinien verwendet werden, überprüfen Sie die folgenden Einstellungen für das Konto. Führen Sie den Gruppenrichtlinieneditor „gpedit.msc“ aus und informieren Sie sich unter **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten**.

- Lokal anmelden verweigern – Fügen Sie das Konto nicht hinzu.
- Lokal anmelden zulassen – Fügen Sie das Konto hinzu.
- Zugriff vom Netzwerk auf diesen Computer verweigern – Fügen Sie das Konto nicht hinzu.
- Auf diesen Computer vom Netzwerk aus zugreifen – Fügen Sie das Konto hinzu.

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 Domänennamen (FQDN) auflösen können.

Geben Sie bei der Installation stets den vollqualifizierten Domänennamen (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 Datenübertragungsrate 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 AutomationReplikat-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.

VMware unterstützt keine Appliance-Änderungen oder -Anpassungen. Fügen Sie Pakete oder benutzerdefinierte Skripts niemals hinzu und entfernen oder aktualisieren Sie sie niemals.

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 2-1. 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 2-2. Eingehende Ports

Port	Protokoll	Anmerkungen
22	TCP	Optional. Zugriff auf SSH-Sitzungen.
80	TCP	Optional. Leitet weiter zu 443.
88	TCP (UDP optional)	Cloud KDC-Kerberos-Authentifizierung von externen mobilen Geräten.

Tabelle 2-2. Eingehende Ports (Fortsetzung)

Port	Protokoll	Anmerkungen
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.
8494	TCP	Synchronisierung des Container-Dienstclusters
9300–9400	TCP	Zugriff für Identity Manager-Audits.
54328	UDP	
40002, 40003	TCP	Synchronisierung des vIDM-Clusters
8090, 8092	TCP	Wird vom Integritätsdienst zum Herstellen einer Verbindung zwischen vRA-Knoten verwendet

Tabelle 2-3. 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.

Tabelle 2-3. Ausgehende Ports (Fortsetzung)

Port	Protokoll	Anmerkungen
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.
		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.
8494	TCP	Synchronisierung des Container-Dienstclusters
9300–9400	TCP	Zugriff für Identity Manager-Audits.
54328	UDP	
40002, 40003	TCP	Synchronisierung des vIDM-Clusters

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.

Wichtig Die Installation deaktiviert Windows-Firewall. Wenn für die Site-Richtlinien Windows-Firewall erforderlich sind, aktivieren Sie sie nach der Installation erneut und öffnen Sie die IaaS-Windows Serverports einzeln. Weitere Informationen finden Sie unter [Ports auf IaaS-Windows-Servern](#).

- 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.

- IaaS-Windows-Server und der SQL Server-Datenbankhost müssen in der Lage sein, sich gegenseitig anhand des NETBIOS-Namens aufzulösen. Fügen Sie bei Bedarf die NETBIOS-Namen der Datei /etc/hosts auf jedem IaaS-Windows-Server und dem SQL Server-Datenbankhost hinzu und starten Sie die Maschinen neu.
- 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 verwendeter Windows-Version Microsoft PowerShell 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.
- Legen Sie IaaS-Windows-Server für alle Bereitstellungen außer Minimalbereitstellungen auf das englische Gebietsschema fest.

- 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 2-4. 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 2-4. 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 2-5. 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.

laaS-Webserver

Ein Windows-Server, der die Webkomponente hostet, muss neben den für alle laaS 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 191 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 2-6. IaaS-Internetinformationsdienste

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"> ■ Anbieteraushandlung 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.

Zwischen einem Manager Service-Host und einem DEM-Host dürfen keine Firewalls vorhanden sein. Portinformationen finden Sie unter [Ports auf IaaS-Windows-Servern](#).

Die Anforderung ist identisch, ganz gleich, ob es sich bei dem Manager Service-Host um einen primären oder einen Backup-Host handelt.

laaS SQL Server-Host

Ein Windows-Server, der die laaS SQL-Datenbank hostet, muss bestimmte Anforderungen erfüllen.

Ihr SQL Server kann sich auf einem Ihrer laaS Windows-Server oder auf einem separaten Host befinden. Wenn dieser gemeinsam mit laaS-Komponenten gehostet wird, müssen neben diesen für alle laaS 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 laaS erstellen, verwenden Sie den Kompatibilitätsmodus 100 oder 120.

Wenn Sie die Datenbank mit dem vRealize Automation-Installationsprogramm erstellen, ist die Kompatibilität bereits konfiguriert.

Dasselbe Verhalten gilt auch für SQL Server 2017.

- AlwaysOn-Verfügbarkeitsgruppe (AlwaysOn Availability Group, AAG) wird nur für SQL Server 2016 Enterprise oder SQL Server 2017 Enterprise unterstützt. Bei Verwendung von AAG geben Sie den AAG-Listener-FQDN als SQL-Server-Host an. Legen Sie beim Erstellen von AAG DTC_Support = Per_DB fest. Das Festlegen nach der Erstellung von AAG funktioniert nicht.
- Wenn der SQL Server gemeinsam mit laaS-Komponenten gehostet wird, konfigurieren Sie Java.
 - Installieren Sie Java 1.8, 64 Bit, Update 181 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 laaS ordnungsgemäß installiert wird, ändern Sie nicht die Größe der Modelldatenbank.
- Im Gegensatz zu den in [laaS-Windows-Server](#) aufgeführten Minimalanforderungen benötigt der Server in der Regel mehr Hardware.

Weitere Informationen finden Sie unter *Hardwarespezifikationen und maximale Kapazitäten* im vRealize Automation *Referenzarchitektur-Handbuch*.

- 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 2-7. 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 AutomationIaaS 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-verwandten 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 der 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 Ihrer SCVMM-Umgebung finden Sie unter *Konfigurieren von vRealize Automation*.

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 Bereitstellungsvorgangs 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 2-8. 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	2048, 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-PKCS1_V1_5			
Schlüssellänge	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-PKCS1_V1_5			
Schlüssellänge	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 für die virtuellen Appliances müssen im PEM-Format vorliegen.

Wenn Ihre Zertifizierungsstelle ein Zertifikat im PFX-Format bereitgestellt hat, verwenden Sie OpenSSL, um PFX in PEM zu konvertieren.

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

Beispiel:

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

Sie werden möglicherweise aufgefordert, eine Passphrase einzugeben, wenn das PFX-Zertifikat eines enthielt.

Bereitstellen der vRealize Automation-Appliance

3

Die vRealize Automation-Appliance wird als offene Virtualisierungsdatei geliefert, die Sie in einer vorhandenen virtualisierten Infrastruktur bereitstellen.

Dieses Kapitel enthält die folgenden Themen:

- [Informationen zur Bereitstellung der vRealize Automation-Appliance](#)
- [Bereitstellen der vRealize Automation-Appliance](#)
- [Hinzufügen von Netzwerkkarten vor Ausführung des Installationsprogramms](#)

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 3-1. 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 it later 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 a static IP. 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 later (by 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 hinzufügen.

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 PostgreSQL-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-addressnetmaskgateway-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

4

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 [Kapitel 5 Die vRealize Automation-Standard-Installationsschnittstellen](#).

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden des Installationsassistenten für minimale Bereitstellungen](#)
- [Verwenden des Installationsassistenten für Unternehmensbereitstellungen](#)

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 [Kapitel 2 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 4-1. Management-Agent – Details zur vRealize Automation-Appliance

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.

Ergebnisse

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 [Kapitel 6 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.
- 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 Mandantenadministratoren müssen die Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren, wenn sie den Link zu Active Directory konfigurieren.

Voraussetzungen

- Sorgen Sie dafür, dass die in [Kapitel 2 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 primären 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 primären 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 oder -Appliances 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 primären 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 primäre 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 primären vRealize Automation-Appliance ein.

- a Geben Sie die HTTPS-Adresse der primären Appliance einschließlich FQDN und :5480-Portnummer ein.
- b Geben Sie die Anmeldedaten für das Root-Konto der primären 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 4-2. Management-Agent – Details zur vRealize Automation-Appliance

- 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.

Ergebnisse

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 [Kapitel 6 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.
- Informationen zum Konfigurieren des Zugriffs auf den Standardmandanten finden Sie unter [Konfigurieren des Zugriffs auf den Standardmandanten](#).

Die vRealize Automation-Standard-Installationsschnittstellen

5

Nachdem der Installationsassistent ausgeführt wurde, müssen oder möchten Sie möglicherweise bestimmte Installationsaufgaben manuell über die Standardschnittstellen durchführen.

Der unter [Kapitel 4 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.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden der Standardschnittstellen für minimale Bereitstellungen](#)
- [Verwenden der Standardschnittstellen für verteilte Bereitstellungen](#)
- [Installieren der vRealize Automation-Agents](#)

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 5-1. Checkliste für Minimalbereitstellung

Aufgabe	Details
<input type="checkbox"/> Planen Sie die Umgebung und sorgen Sie dafür, dass die Installationsvoraussetzungen erfüllt sind.	Kapitel 2 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 > 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-loadbalancename.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 über das Menü **Zertifikatsaktion** die gewünschte Aktion aus.

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

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

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

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

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

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

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

- 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 > 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** 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.

Ergebnisse

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 AutomationIaaS](#)

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. XenServer 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 AutomationIaaS

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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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**.

Ergebnisse

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 Domänennamen 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 **laaS-Server**, der den Hostnamen der Windows-Maschine enthält, auf der Sie die Installation durchführen.
 - 8 Klicken Sie auf den Testlink rechts vom Feld **laaS-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 laaS-Installation ab.

Voraussetzungen

- [Registrieren der laaS-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 laaS-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**.

Ergebnisse

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 5-2. Checkliste für die verteilte Bereitstellung

Aufgabe	Details
<input type="checkbox"/> Planen und Vorbereiten der Installationsumgebung und Überprüfen, ob alle Installationsvoraussetzungen erfüllt sind.	Kapitel 2 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

Tabelle 5-2. Checkliste für die verteilte Bereitstellung (Fortsetzung)

Aufgabe	Details
<input type="checkbox"/> Konfigurieren Ihres Lastausgleichsdiensts für die Bewältigung des Datenverkehrs der vRealize Automation-aaS-Komponente und Installieren der vRealize Automation-aaS-Komponenten.	Installieren der AaaS-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 der AaaS-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 *Verwenden des 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.

Weitere Informationen zum Konfigurieren der Verzeichnisverwaltung für Hochverfügbarkeit finden Sie im Handbuch *Konfigurieren von vRealize Automation*.

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 AaaS-Webserver sowie mehrere AaaS-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 geclusterten Bereitstellung folgt die Zertifikatsorganisation weitgehend der dreistufigen vRealize Automation-Architektur.

- vRealize Automation-Appliances
- IaaS-Webkomponenten
- IaaS Manager Service-Komponenten

In einer verteilten Bereitstellung teilen sich alle Maschinen einer bestimmten Ebene ein Zertifikat. Beispielsweise teilt jede vRealize Automation-Appliance ein gemeinsames Zertifikat, und jeder Manager Service-Host teilt ein gemeinsames Zertifikat.

Wenn die Web- und Manager Service-Komponenten auf derselben Maschine gehostet werden, reicht ein Zertifikat für beide Ebenen aus.

Vom System generierte Zertifikate

Wenn Sie ab Version 7.0 keine eigenen Zertifikate bereitstellen, kann der vRealize Automation-Installationsassistent automatisch selbstsignierte Zertifikate generieren und sie in den entsprechenden Trust Stores auf den verteilten Komponenten, die sie benötigen, ablegen.

Wenn Sie vom System generierte selbstsignierte Zertifikate mit vom Benutzer oder der Zertifizierungsstelle bereitgestellten Zertifikaten aktualisieren müssen, finden Sie weitere Informationen unter *Verwalten von vRealize Automation*.

Bereitstellen eigener Zertifikate

Wenn Sie das standardmäßige, manuelle Installationsprogramm ausführen, stellen Sie die von Ihnen selbst generierten selbstsignierten Zertifikate oder Zertifizierungsstellenzertifikate bereit.

Wenn Sie eigene Zertifikate bereitstellen oder mit OpenSSL oder einer anderen Methode generieren, können Sie entweder Platzhalter- oder SAN-Zertifikate (Subject Alternative Name) verwenden.

IaaS-Zertifikate müssen mehrfach verwendbare Zertifikate sein. Falls Sie Zertifikate bereitstellen, müssen Sie ein mehrfach verwendbares Zertifikat anfordern, das die IaaS-Komponenten im Cluster enthält, und dieses Zertifikat dann in den Trust Store jeder Komponente kopieren.

Lastausgleichsdienste

Für Hochverfügbarkeit und Failover können Sie Lastausgleichsdienste vor verteilten vRealize Automation-Komponenten hinzufügen. VMware empfiehlt eine Passthrough-Konfiguration für vRealize Automation-Lastausgleichsdienste. In einer Passthrough-Konfiguration übergeben Lastausgleichsdienste Anforderungen an Komponenten ohne Entschlüsselung. Die vRealize Automation-Appliances und IaaS-Hosts führen dann die erforderliche Entschlüsselung durch.

Wenn Sie Lastausgleichsdienste verwenden, müssen Sie den FQDN für den Lastausgleichsdienst in der vertrauenswürdigen Adresse von mehrfach verwendbaren Zertifikaten des Clusters angeben.

Weitere Informationen zum Verwenden und Konfigurieren von Lastausgleichsdiensten finden Sie unter *vRealize Automation-Lastausgleich*.

Anforderungen an vertrauenswürdige Zertifikate

Die folgende Tabelle enthält eine Übersicht über die Registrierungsanforderungen der Vertrauensstellung für verschiedene importierte 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
IaaS Manager Service-Komponentencluster	<ul style="list-style-type: none"> ■ DEM-Orchestrator- und DEM-Worker-Komponenten ■ Agents und Proxy-Agents

Zertifikatvertrauensstellung und Standardinstallationsprogramm

Immer wenn Sie das standardmäßige, manuelle Installationsprogramm zum Erstellen von IaaS-Komponenten ausführen oder erneut ausführen, müssen Sie die Zertifikatvertrauensstellung für diese IaaS-Komponenten konfigurieren. Beispielsweise können Sie das Standardinstallationsprogramm verwenden, um eine vorhandene Bereitstellung horizontal zu skalieren.

- IaaS-Web- und Manager Service-Hosts

Importieren Sie die Dateien `web.pfx` und `ms.pfx` an die folgenden Speicherorte.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

- IaaS-DEM-Orchestrator, -DEM-Worker und Proxy-Agent-Hosts

Importieren Sie die Dateien `web.pfx` und `ms.pfx` an den folgenden Speicherort.

```
Host Computer/Certificates/Trusted People certificate store
```

Im Zertifikatspeicher für vertrauenswürdige Personen müssen Sie den privaten Schlüssel nicht zusammen mit dem Zertifikat importieren. Beim automatischen Installationsvorgang wird nur das Zertifikat im Zertifikatspeicher für vertrauenswürdige Personen installiert.

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 5-3. vRealize Automation-Appliance

Variable	Mein Wert	Beispiel
FQDN der primären vRealize Automation-Appliance		automation.mycompany.com
IP-Adresse der primären vRealize Automation-Appliance Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.105
FQDN der zusätzlichen vRealize Automation-Appliance		automation2.mycompany.com
IP-Adresse der zusätzlichen vRealize Automation-Appliance Nur als Referenz, geben Sie keine IP-Adressen ein.		123.234.1.106
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://appliance-FQDN:5480) der Verwaltungsschnittstelle	Root (Standard)	root
Kennwort der Verwaltungsschnittstelle		admin123
Standardmandant	vsphere.local (Standard)	vsphere.local

Tabelle 5-3. vRealize Automation-Appliance (Fortsetzung)

Variable	Mein Wert	Beispiel
Standardbenutzername des Mandanten	administrator@vsphere.local (Standard)	administrator@vsphere.local
Standardkennwort des Mandanten		login123

Tabelle 5-4. 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
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

Tabelle 5-4. IaaS-Windows-Server (Fortsetzung)

Variable	Mein Wert	Beispiel
Für IaaS-Dienste, Domänenkonto mit Administratorrechten auf Hosts		SUPPORT\provisioner
Kontokennwort		login123

Tabelle 5-5. IaaS-SQL Server-Datenbank

Variable	Mein Wert	Beispiel
Datenbankinstanz		IAASSQL
Datenbankname	vcac (Standard)	vcac
Passphrase (wird bei Installation, Upgrade und Migration verwendet)		login123

Tabelle 5-6. 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 im technischen Whitepaper *Konfigurationshandbuch für den 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 > 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-loadbalancename.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 über das Menü **Zertifikatsaktion** die gewünschte Aktion aus.

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

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

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

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

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

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

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

- 6 Klicken Sie auf **Einstellungen speichern**, um Hostinformationen und SSL-Konfiguration zu speichern.
- 7 Falls Ihr Netzwerk oder Lastenausgleichsdienst dies erfordert, kopieren Sie das importierte oder neu erstellte Zertifikat in den Lastenausgleichsdienst 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 Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.

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

- 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 > 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 Klicken Sie auf **Messaging**. Die Konfigurationseinstellungen und der Status des Messaging für Ihre Appliance werden angezeigt. Ändern Sie diese Einstellungen nicht.

12 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.

13 Klicken Sie auf **Einstellungen speichern**.

14 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.

Active Directory – Jede vRealize Automation-Appliance enthält einen Connector, der die Benutzerauthentifizierung unterstützt, jedoch ist in der Regel nur ein Connector zum Ausführen der Verzeichnissynchronisierung konfiguriert. Denken Sie nach dem Hinzufügen einer weiteren Appliance daran, einen zweiten Connector zu konfigurieren, der der hinzugefügten Appliance entspricht. Der zweite Connector stellt eine Verbindung mit dem Identitätsanbieter her und verweist auf dasselbe Active Directory. Wenn die erste Appliance ausfällt, übernimmt die zweite die Verwaltung der Benutzerauthentifizierung.

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 > 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.

Ergebnisse

Wenn ein Clusterbeitrittsvorgang sehr viel Zeit in Anspruch nimmt und schließlich abläuft, finden Sie weitere Informationen im [VMware-Knowledgebase-Artikel 58708](#).

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 Lastausgleichsdienstadresse 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 Webserver 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 AutomationIaaS](#).

Herunterladen des Installationsprogramms für vRealize AutomationIaaS

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 Zertifikatstamm 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 5-7. 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 Skripten 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-Datenbankinstallationsskripte 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 ALLOW_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 5-8. Datenbankwerte

Variable	Wert
<i>db_server</i>	Gibt die SQL Server-Instanz im Format dbhostname[,port number]\SQL instance 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 localhost.
<i>db_name</i>	Der Name der Datenbank. Der Standardwert lautet vra. 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.
<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.

Ergebnisse

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 5-9. Datenbankwerte

Variable	Wert
\$(DBName)	Name der Datenbank, wie beispielsweise vra. Datenbanknamen dürfen aus maximal 128 ASCII-Zeichen bestehen.
\$(DBDir)	Der Pfad zum Datenverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
\$(LogDir)	Der Pfad zum Protokollverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.

- 5 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.

- 6 Öffnen Sie SQL Server Management Studio.

- 7 Klicken Sie auf **Neue Abfrage**.

Es wird ein Fenster zur SQL-Abfrage geöffnet.

- 8 Stellen Sie im Menü **Abfrage** sicher, dass **SQLCMD-Modus** ausgewählt ist.

- 9 Fügen Sie den gesamten geänderten Inhalt von `CreateDatabase.sql` in das Abfragefenster ein.

- 10 Fügen Sie unter dem Inhalt von `CreateDatabase.sql` den gesamten geänderten Inhalt von `SetDatabaseSettings.sql` hinzu.

- 11 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 **IaaS-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 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 Wählen Sie auf der Seite für die benutzerdefinierte Installation von IaaS 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 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](#).

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**.

Ergebnisse

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.

Ergebnisse

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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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** und **ModelManagerData** 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-Zertifikatssperrlisten.

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 in 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* im Handbuch *Verwalten von vRealize Automation*.
- 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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-Zertifikatssperrlisten.

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 Dienstkontobenzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenzers 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 **IaaS-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 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 Wählen Sie **Manager Service** auf der Seite **Benutzerdefinierte Installation des IaaS-Servers** aus.
- 11 Identifizieren Sie im Textfeld **IaaS-Server** die IaaS-Webserver-Komponente.

Option	Beschreibung
Wenn Sie einen Lastenausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastenausgleichsdiensts für die IaaS-Webserver-Komponente ein (<i>web-load-balancer.mycompany.com:443</i>). Geben Sie keine IP-Adressen ein.
Wenn Sie keinen Lastenausgleichsdienst verwenden	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die IaaS 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 Lastenausgleichsmodule 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 Dienstkontobenzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenzers 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* im Handbuch *Verwalten von vRealize Automation*.
- 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 **Manager Service** auf der Seite **Benutzerdefinierte Installation des laaS-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 IaaS-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 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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.

Ergebnisse

Weitere Informationen finden Sie unter [DEM-Worker mit SCVMM](#).

Weitere Informationen zur Vorbereitung der SCVMM-Umgebung und der Erstellung eines SCVMM-Endpoints finden Sie unter *Konfigurieren von vRealize Automation*.

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 VMPSOpsUser.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 VMPSOpsUser.sql in das Abfragefenster ein.
- 9 Klicken Sie auf **Ausführen**.

Ergebnisse

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 5-10. Auswählen eines Agent-Szenarios

Integrationsszenario	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

Tabelle 5-10. Auswählen eines Agent-Szenarios (Fortsetzung)

Integrationsszenario	Agent-Anforderungen und Vorgehensweisen
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-Skripten 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\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.

Mit dem Recht `VApp.Import` können Sie eine vSphere-Maschine bereitstellen, indem Sie die aus einer OVF-Datei importierten Einstellungen importieren. Details zu diesem vSphere-Recht finden Sie in der [vSphere SDK-Dokumentation](#). Wenn Sie einen vSphere-Endpoint zum Bereitstellen von VMs über OVF-Vorlagen verwenden möchten, stellen Sie sicher, dass Ihre Anmeldedaten das vSphere-Recht `VApp.Import` auf dem vCenter Server enthalten, der mit dem Endpoint verknüpft ist.

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 5-11. 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
vApp		Importieren
		vApp-Anwendungskonfiguration
Ressourcen		Ressourcenpool VMs zuweisen
		Ausgeschaltete virtuelle Maschine migrieren
		Eingeschaltete virtuelle Maschine migrieren
Virtuelle Maschine	Bestandsliste	Aus vorhandener erstellen
		Neue erstellen
		Verschieben

Tabelle 5-11. Erforderliche Berechtigungen an vSphere-Agents für die Verwaltung von vCenter Server-Instanzen (Fortsetzung)

Attributwert	Berechtigung
Interaktion	Entfernen
	CD-Medien konfigurieren
	Konsoleninteraktion
	Geräteverbindung
	Ausschalten
	Einschalten
	Zurücksetzen
	Anhalten
	Tools installieren
	Vorhandene Festplatte hinzufügen
	Neue Festplatte hinzufügen
	Gerät hinzufügen oder entfernen
	Festplatte entfernen
	Erweitert
	CPU-Anzahl ändern
	Ressourcen ändern
	Virtuelle Festplatte erweitern
	Festplattenänderungsverfolgung
	Arbeitsspeicher
Konfiguration	Geräteeinstellungen ändern
	Umbenennen
	Anmerkung festlegen (Version 5.0 und höher)
	Einstellungen
	Platzierung der Auslagerungsdatei
	Anpassen
	Vorlage klonen
	Virtuelle Maschine klonen
	Vorlage bereitstellen

Tabelle 5-11. Erforderliche Berechtigungen an vSphere-Agents für die Verwaltung von vCenter Server-Instanzen (Fortsetzung)

Attributwert	Berechtigung
	Anpassungsspezifikationen lesen
Zustand	Snapshot erstellen
	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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 AutomationHyper-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 AutomationIaaS](#).
- 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 Domänennamen identifiziert werden müssen.

vRealize Automation kann nicht mit einem Knoten kommunizieren bzw. keinen Knoten verwalten, der nicht durch seinen vollqualifizierten Domänennamen innerhalb des Xen-Pools identifiziert wird.
- Konfigurieren Sie Hyper-V für Remoteverwaltung, um die Hyper-V-Serverkommunikation mit vRealize AutomationHyper-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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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: XSadmin
```

- 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 Domänennamen (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 AutomationIaaS](#).

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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 AutomationIaaS](#).

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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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

Installationsverzeichnis 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/VBScripts-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 5-12. 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-Skripts als zusätzliche Schritte beim Bereitstellungsvorgang.

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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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 Verwaltungsschnittstelle der vRealize Automation-Appliance 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

6

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.

Dieses Kapitel enthält die folgenden Themen:

- [Informationen zur automatischen Installation von vRealize Automation](#)
- [Ausführen einer automatischen vRealize Automation-Installation](#)
- [Ausführen einer automatischen Installation des vRealize Automation-Management-Agents](#)
- [Antwortdatei der unbeaufsichtigten vRealize Automation-Installation](#)
- [Die vRealize Automation-Installationsbefehlszeile](#)
- [Die vRealize Automation-Installations-API](#)
- [Konvertierung von vRealize Automation-Eigenschaften der automatischen Installation in JSON](#)

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 Texteditor 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 Installationsskripts 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-IDBefehlsname --ParameternameParameterwert
```

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`

Ergebnisse

Sie können auch die Hilfe für das Skript anzeigen.

`/usr/lib/vcac/tools/install/convert-properties --help`

vRealize Automation-Aufgaben nach der Installation

7

Nach der Installation von vRealize Automation müssen Sie sich möglicherweise um Aufgaben nach der Installation kümmern.

Dieses Kapitel enthält die folgenden Themen:

- [Keine Änderung der vRealize Automation-Zeitzone](#)
- [Konfigurieren der Federal Information Processing Standard-konformen Verschlüsselung](#)
- [Aktivieren des automatischen Manager Service-Failovers](#)
- [Automatisches Failover der PostgreSQL-Datenbank von vRealize Automation](#)
- [Ersetzen von selbstsignierten Zertifikaten mit von einer Zertifizierungsstelle bereitgestellten Zertifikaten](#)
- [Ändern von Hostnamen und IP-Adressen](#)
- [Entfernen eines Knotens der vRealize Automation-Appliance](#)
- [Installieren des vRealize Log Insight-Agents auf IaaS-Servern](#)
- [Ändern des VMware Remote Console-Proxy-Ports](#)
- [Ändern eines vRealize Automation-Appliance-FQDN in den ursprünglichen FQDN](#)
- [Konfigurieren von SQL AlwaysOn Availability Group](#)
- [Hinzufügen von Netzwerkkarten nach der Installation von vRealize Automation](#)
- [Konfigurieren von statischen Routen](#)
- [Zugriff auf Patch-Verwaltung](#)
- [Konfigurieren des Zugriffs auf den Standardmandanten](#)

Keine Änderung der vRealize Automation-Zeitzone

Auch wenn in der Verwaltungsschnittstelle der vRealize Automation-Appliance eine Option zum Ändern zur Verfügung steht, behalten Sie für die vRealize Automation-Zeitzone immer die Einstellung „Etc/UTC“ bei.

Die Verwendung einer anderen Zeitzone als Etc/UTC führte bereits zu ungewöhnlichen Fehler, wie z. B. fehlgeschlagene Migrationen und Protokollpakete, die keine Einträge aus allen vRealize Automation-Knoten enthalten.

Die zu vermeidende Verwaltungsschnittstellenoption der vRealize Automation-Appliance befindet sich unter **System > Zeitzone**.

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 > 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.

Ergebnisse

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.

In einer Konfiguration mit mehreren Knoten müssen Sie die Schritte nur einmal auf jedem vRealize Automation-Appliance-Knoten ausführen.

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
```

Ergebnisse

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 *Upgrade von vRealize Automation 7.1 oder 7.2 auf 7.3* Tipps zur Fehlerbehebung.

Informationen zum Lastausgleich für Manager Service-Hosts finden Sie unter [vRealize Automation-Lastausgleichsdienst](#).

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 Datenbankreplikierung ist auf der Registerkarte „Cluster“ der vRealize Automation-Verwaltungsschnittstelle auf „Synchroner Modus“ eingestellt.

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 zum Durchführen eines manuellen Failovers finden Sie unter *Verwalten von vRealize Automation*.

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 *Verwalten von vRealize Automation*.

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 im Handbuch *Verwalten von vRealize Automation*.
- 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.

Ergebnisse

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**.
- 4 Erweitern Sie **OVF-Einstellungen** und aktivieren Sie die Option **ISO-Image**.

Virtual Hardware	VM Options	SDRS Rules	vApp Options
<div>▼ IP allocation</div> <div>IP allocation scheme</div> <p>A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp:</p> <p><input type="checkbox"/> DHCP</p> <p><input checked="" type="checkbox"/> OVF environment</p> <p>The IP allocation schemes determine what IP allocation policy options are enabled.</p> <div>IP protocol</div> <p>Specify the IP protocols supported by this vApp:</p> <p>Both</p>			
<div>▼ OVF settings</div> <div>OVF environment</div> <p>View...</p> <p>The OVF environment is only available when the VM is powered on.</p> <div>OVF environment transport</div> <p><input checked="" type="checkbox"/> ISO image</p> <p>An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive.</p> <p><input checked="" type="checkbox"/> VMware Tools</p> <p>The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document.</p> <div>Installation boot</div> <p><input type="checkbox"/> Enable</p> <p>The installation boot automatically gets reset upon first power-on of the virtual machine.</p> <p>0</p> <p>Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off</p>			

- 5 Klicken Sie auf **OK**.
- 6 Starten Sie die vRealize Automation-Appliance, die Sie ändern.
- 7 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
`https://vrealize-automation-appliance-FQDN:5480`
- 8 Klicken Sie auf die Registerkarte **Netzwerk**.
- 9 Klicken Sie unter den Registerkarten auf **Adresse**.

- 10 Aktualisieren Sie die IP-Adresse.
- 11 Klicken Sie oben rechts auf **Einstellungen speichern**.
- 12 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.
 - Datenbank-Verbindungsstatus unter **Cluster**
 - RabbitMQ-Status unter **vRA > Messaging**
 - Xenon-Status unter **vRA > 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.
Informationen zum Aktualisieren von Zertifikaten finden Sie unter *Verwalten von vRealize Automation*.

- 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 Lastausgleichdiensts finden, behalten Sie diesen Namen bei.

Tabelle 7-1. Dateien, die aktualisiert werden müssen, wenn Sie den Hostnamen eines Web-Knotens ändern

IaaS-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>	Repoutil.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 7-2. Dateien, die aktualisiert werden müssen, wenn Sie den Hostnamen eines Manager Service-Knotens ändern

IaaS-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 7-3. 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 > Hosteinstellungen** den **Hostnamen** in den ausgewählten CNAME-Eintrag.

Entfernen eines Knotens der vRealize Automation-Appliance

Bei der Wartung einer HA-Umgebung müssen Sie möglicherweise einen fehlerhaften Knoten der vRealize Automation-Appliance aus dem Cluster entfernen.

Befolgen Sie zum Entfernen eines Knotens die Richtlinien im [VMware-Knowledgebase-Artikel 2149866](#).

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 im *VMware vRealize Log Insight Agent-Administratorhandbuch*. 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.

Ergebnisse

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 dazu finden Sie unter *Konfigurieren von vRealize Automation*.

- 2 Wenn es sich um eine HA-Umgebung handelt, befolgen Sie auch die Schritte zum Konfigurieren der Verzeichnisverwaltung für HA in *Konfigurieren von vRealize Automation*.
- 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="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

In:

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="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 > Messaging** und klicken Sie auf **RabbitMQ-Cluster zurücksetzen**.
- 7 Melden Sie sich nach dem Zurücksetzen bei jeder Appliance-Verwaltungsschnittstelle an.
- 8 Wechseln Sie zu **Cluster** und vergewissern Sie sich, 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 7-4. 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.

Da nahezu in Echtzeit Probleme auftreten können, werden in der [VMware-Knowledgebase](#) Patches, Voraussetzungen und Installationsanweisungen veröffentlicht. Beispielsweise wird der [Artikel 60310 der VMware-Knowledgebase](#) überwacht und mit den neuesten vRealize Automation 7.5-Patch-Informationen aktualisiert.

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

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 > 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
```

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. Siehe *Konfigurieren von vRealize Automation*.
- Ihre IaaS-Administratoren bereiten externe Ressourcen für die Bereitstellung vor. Siehe *Konfigurieren von vRealize Automation*.
- 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.

Fehlerbehebung bei einer vRealize Automation-Installation

8

Die Fehlerbehebung bei vRealize Automation beschreibt Verfahren zur Lösung von Problemen, die bei der Installation oder Konfiguration von vRealize Automation auftreten können.

Dieses Kapitel enthält die folgenden Themen:

- [Standardspeicherorte für Protokolle](#)
- [Rollback einer fehlgeschlagenen Installation wird ausgeführt](#)
- [Erstellen eines vRealize Automation-Support-Pakets](#)
- [Allgemeine Fehlerbehebung bei der Installation](#)
- [Fehlerbehebung bei der vRealize Automation-Appliance](#)
- [Fehlerbehebung bei IaaS-Komponenten](#)
- [Fehlerbehebung bei Anmeldefehlern](#)

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 Sie AaaS 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.

Ergebnisse

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.

Ergebnisse

Tabelle 8-1. 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.

Tabelle 8-1. Rollback-Fehlerpunkte (Fortsetzung)

Fehlerpunkt	Aktion
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 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 > Protokolle**.
- 3 Klicken Sie auf **Support-Paket erstellen**.
- 4 Klicken Sie auf **Herunterladen** und speichern Sie die Support-Paket-Datei auf Ihrem System.

Ergebnisse

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.

Befehlszeile – Um ein Support-Paket über die Befehlszeile der vRealize Automation-Appliance als Root zu generieren, können Sie `vcac-support` oder `vcac-config log-bundle` ausführen.

Alternativ können Sie den vollständigen log-bundle-Befehl ausführen, wie im folgenden Beispiel gezeigt. Allgemeine Informationen zum Ausführen von `vra-command` finden Sie unter [Grundlagen für die Installation von vRealize Automation über die Befehlszeile](#).

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

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.

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).

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

- 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.

Lösung

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.

Voraussetzungen

Bitten Sie den Administrator der Site, Ihnen Proxy-Servernamen, Portnummern und Anmeldedaten bereitzustellen.

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

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

`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.

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.

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

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/workflowexecutor.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/workflowexecutor.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.

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.

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 Besitzerbenutzerebene ist nicht ordnungsgemäß zugewiesen.

Lösung

- 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-Datenverwaltungsprogramm 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, lockedby=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 Verwaltungsschnittstelle 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 „Cluster“ in der Verwaltungsschnittstelle dieses Knotens wird dieser weiterhin als Master-Knoten aufgeführt, obwohl er es nicht ist. Versuche, das Problem über die Verwaltungsschnittstelle 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 Verwaltungsschnittstelle des neuen Master-Knotens. Suchen Sie nach dem alten Knoten, der auf der Registerkarte „Cluster“ 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 Verwaltungsschnittstelle 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.
- Der SQL-Dienst wird möglicherweise nicht ausgeführt.

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-Lastausgleichsdienst-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-Web-server-or-load-balancer-IP-or-FQDN /vcac
--Endpoint ui -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI
--Endpoint wapi -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-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
```

- 7 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.

Distributed Transaction Coordinator-Verbindungen werden abgelehnt

Die RPC-Einstellungen (Remote Procedure Call, Remoteprozeduraufruf) von Microsoft können sich auf Distributed Transaction Coordinator (DTC) in vRealize Automation auswirken.

Problem

Es treten Fehler auf, die angeben, dass DTC-Verbindungen zwischen IaaS-Windows-Servern oder dem vRealize Automation-SQL-Datenbankserver abgelehnt werden.

Ursache

Eine RPC-Verbindungseinstellung schränkt den Zugriff ein und muss deaktiviert werden.

Lösung

Entfernen Sie auf allen IaaS-Windows-Servern und dem vRealize Automation-SQL-Datenbankserver den folgenden Registrierungsschlüssel oder setzen Sie ihn auf Null.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients

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 Befehl 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 Domänennamen 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 msixec-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-Zertifikatssperrlisten 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 `%SystemDrive%\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 *cODDOC01*.

- 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.

- 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 Serverinstallationsverzeichnisses 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.

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.

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

- ◆ 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 Domänennamen 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.

Voraussetzungen

Konfigurieren Sie vRealize Automation für den Zugriff auf das Netzwerk über einen Proxyserver. Siehe [Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server](#).

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

- 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`