

# Installieren von vRealize Automation

vRealize Automation 7.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter

<http://www.vmware.com/de/support/pubs>.

DE-002088-04

**vmware**<sup>®</sup>

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

<http://www.vmware.com/de/support/>

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2017 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

**VMware, Inc.**

3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Global, Inc.**

Zweigniederlassung Deutschland  
Freisinger Str. 3  
85716 Unterschleißheim/Lohhof  
Germany  
Tel.: +49 (0) 89 3706 17000  
Fax: +49 (0) 89 3706 17333  
[www.vmware.com/de](http://www.vmware.com/de)

# Inhalt

vRealize Automation -Installation	7
Aktualisierte Informationen	9
<b>1 Überblick über die vRealize Automation -Installation</b>	<b>11</b>
Auswählen des Bereitstellungspfads	11
Überblick über Minimalbereitstellung	13
Übersicht über die Unternehmensbereitstellung	13
vRealize Automation -Installationskomponenten	15
Die vRealize Automation -Appliance	15
Management-Agents	15
vRealize Automation Infrastructure-as-a-Service	15
<b>2 Vorbereitung für die Installation von vRealize Automation</b>	<b>19</b>
Hostnamen und IP-Adressen	19
Anforderungen an die Hardware und an virtuelle Maschinen	20
Überlegungen zum Browser	20
Überlegungen zum Kennwort	21
Anforderungen an Windows Server	21
IaaS -Datenbankserveranforderungen	21
Anforderungen an den IaaS-Webdienst und den Model Manager-Server	22
IaaS Manager Service	23
Anforderungen an den Distributed Execution Manager	23
vRealize Automation -Portanforderungen	26
Für die Installation erforderliche Benutzerkonten und Anmeldedaten	29
Sicherheit	30
Zertifikate	30
Extrahieren von Zertifikaten und privaten Schlüsseln	31
Sicherheitskennwortsatz	31
Drittanbietersoftware	32
Uhrzeitsynchronisierung	32
<b>3 Installieren von vRealize Automation mit dem Installationsassistenten</b>	<b>33</b>
Bereitstellen der vRealize Automation -Appliance	33
Verwenden des Installationsassistenten für minimale Bereitstellungen	35
Ausführen des Installationsassistenten für eine Minimalbereitstellung	35
Installieren des Management-Agents	36
Synchronisieren der Serveruhrzeit	39
Ausführen der Voraussetzungsprüfung	39
Angaben von Parametern für Minimalbereitstellungen	40
Erstellen von Snapshots vor Beginn der Installation	40
Szenario: Abschließen der Installation	41

Beheben von Installationsfehlern	41
Einrichten der Anmeldedaten für die Erstkonfiguration von Inhalten	42
Verwenden des Installationsassistenten für Unternehmensbereitstellungen	43
Ausführen des Installationsassistenten für eine Unternehmensbereitstellung	43
Installieren des Management-Agents	44
Synchronisieren der Serveruhrzeit	47
Ausführen der Voraussetzungsprüfung	47
Angaben von Parametern für Unternehmensbereitstellungen	48
Erstellen von Snapshots vor Beginn der Installation	48
Abschließen der Installation	49
Beheben von Installationsfehlern	49
Einrichten der Anmeldedaten für die Erstkonfiguration von Inhalten	50
<b>4 Die vRealize Automation -Standard-Installationsschnittstellen</b>	<b>51</b>
Verwenden der Standardschnittstellen für minimale Bereitstellungen	51
Checkliste für Minimalbereitstellung	52
Bereitstellen und Konfigurieren der vRealize Automation -Appliance	52
Installieren der IaaS-Komponenten	58
Verwenden der Standardschnittstellen für verteilte Bereitstellungen	64
Checkliste für die verteilte Bereitstellung	64
Komponenten einer verteilten Installation	65
Deaktivieren der Integritätsprüfungen des Lastausgleichsdiensts	66
Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung	67
Konfigurieren der Webkomponente, des Manager Service und des vertrauenswürdigen DEM-Hostzertifikats	68
Arbeitsblätter zur Installation	68
Bereitstellen der vRealize Automation -Appliance	70
Konfigurieren des Lastausgleichsdiensts	72
Konfigurieren von Appliances für vRealize Automation	72
Installieren der IaaS-Komponenten in einer verteilten Konfiguration	79
Installieren der vRealize Automation -Agents	104
Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned	105
Auswählen des Agent-Installationsszenarios	106
Installationsspeicherort und Anforderungen für Agents	106
Installieren und Konfigurieren des Proxy-Agents für vSphere	106
Installieren des Proxy-Agents für Hyper-V oder XenServer	112
Installieren des VDI-Agents für XenDesktop	116
Installieren des EPI-Agents für Citrix	119
Installieren des EPI-Agents für Visual Basic-Skripterstellung	122
Installieren des WMI-Agents für WMI-Remoteanforderungen	125
<b>5 vRealize Automation -Aufgaben nach der Installation</b>	<b>129</b>
Ersetzen von selbstsignierten Zertifikaten mit von einer Zertifizierungsstelle bereitgestellten Zertifikaten	129
Installieren des vRealize Log Insight -Agents auf IaaS -Servern	129
Konfigurieren des Zugriffs auf den Standardmandanten	129

<b>6</b>	<b>Fehlerbehebung bei einer vRealize Automation -Installation</b>	<b>133</b>
	Standardspeicherorte für Protokolle	133
	Rollback einer fehlgeschlagenen Installation wird ausgeführt	134
	Rollback einer Minimalinstallation ausführen	135
	Rollback einer verteilten Installation ausführen	135
	Erstellen eines vRealize Automation -Support-Pakets	136
	Allgemeine Fehlerbehebung bei der Installation	137
	Installations- oder Aktualisierungsfehler mit einem Zeitüberschreitungsfehler des Lastausgleichsdiensts	137
	Serverzeiten sind nicht synchronisiert	137
	Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 werden möglicherweise leere Seiten angezeigt	138
	Es kann kein Vertrauensverhältnis für den sicheren SSL/TLS-Kanal hergestellt werden	138
	Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server	139
	Konsolenschritte für die Erstkonfiguration von Inhalten	139
	Fehlerbehebung bei der vRealize Automation -Appliance	140
	Installationsprogramme können nicht heruntergeladen werden	140
	Falsche Berechtigungen für die Datei „Encryption.key“	141
	Identity Manager startet nach einem Neustart von horizon-workspace nicht	142
	Falsche Zuweisungen von Appliance-Rollen nach Failover	142
	Fehlerbehebung bei IaaS-Komponenten	143
	Überprüfen der Server-Zertifikate für IaaS	143
	Fehler aufgrund der Anmeldedaten beim Ausführen des IaaS-Installers	144
	Warnung wegen Speicherung der Einstellungen wird während IaaS-Installation angezeigt	144
	Fehler beim Installieren des Website-Servers und der Distributed Execution Manager	144
	IaaS-Authentifizierung schlägt während der Installation der IaaS-Web- und Modellverwaltung fehl	145
	Model Manager-Daten und Webkomponenten können nicht installiert werden	145
	IaaS -Windows-Server unterstützen kein FIPS	146
	Interner Fehler durch Hinzufügen eines XaaS -Endpoints	147
	Ein Proxy-Agent kann nicht deinstalliert werden	147
	Fehler bei Maschinenanforderungen, wenn Remote-Transaktionen deaktiviert sind	148
	Fehler bei der Kommunikation mit dem Manager Service	149
	Geändertes Verhalten für die Anpassung von E-Mails	149
	Fehlerbehebung bei Anmeldefehlern	150
	Anmeldeversuche als IaaS-Administrator mit falsch formatierten UPN-Anmeldedaten schlagen ohne Begründung fehl	150
	Anmeldung schlägt fehl bei Hochverfügbarkeit	150
	Proxy verhindert Anmeldung von VMware Identity Manager-Benutzern	151
<b>7</b>	<b>Hintergrundinstallation von vRealize Automation</b>	<b>153</b>
	Ausführen einer unbeaufsichtigten vRealize Automation -Installation	153
	Ausführen einer unbeaufsichtigten Installation des vRealize Automation -Management-Agents	154
	Antwortdatei der unbeaufsichtigten vRealize Automation -Installation	155
	Die vRealize Automation -Installationsbefehlszeile	156
	Installation von vRealize Automation über die Befehlszeile – Grundlagen	156
	Befehlsnamen für die vRealize Automation -Installation	157



# vRealize Automation -Installation

---

*vRealize Automation-Installation* erklärt, wie VMware vRealize™ Automation installiert wird.

---

**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.

## VMware Technical Publications – Glossar

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





# Aktualisierte Informationen

---

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

Revision	Beschreibung
DE-002088-04	Die Berechtigung „Konfigurieren eines Datenspeicher-Clusters“ wurde in „vSphere Agent-Anforderungen“, auf Seite 107 hinzugefügt.
DE-002088-03	<ul style="list-style-type: none"><li>■ „Konfigurieren des Kontos der Windows-Dienste zur Verwendung von SQL-Authentifizierung“, auf Seite 103 wurde überarbeitet.</li><li>■ „vSphere Agent-Anforderungen“, auf Seite 107 wurde überarbeitet.</li></ul>
DE-002088-02	Updates der Voraussetzungen für IaaS Windows-Server.
DE-002088-01	<ul style="list-style-type: none"><li>■ Zu den ausgehenden IaaS-Ports wurde 5480 hinzugefügt. Siehe „vRealize Automation-Portanforderungen“, auf Seite 26.</li><li>■ Es wurde korrigiert, wohin Sie zum Erstellen eines Support-Pakets navigieren müssen. Siehe „Erstellen eines vRealize Automation-Support-Pakets“, auf Seite 136.</li><li>■ Es wurde die Anforderung des Kompatibilitätsmodus für separate SQL Server-Datenbanken hinzugefügt. Siehe „IaaS-Datenbankserveranforderungen“, auf Seite 21.</li></ul>
DE-002088-00	Erste Produktversion.



# Überblick über die vRealize Automation -Installation

# 1

Sie können vRealize Automation in einer Reihe verschiedener Konfigurationen bereitstellen. Machen Sie sich mit den Bereitstellungs- und Konfigurationsoptionen sowie der Reihenfolge der erforderlichen Aufgaben vertraut, um eine erfolgreiche Bereitstellung sicherzustellen.

Wenn Sie frühere Versionen von vRealize Automation bereitgestellt haben, beachten Sie die folgenden Änderungen, bevor Sie beginnen.

- Diese Version von vRealize Automation umfasst den in vRealize Automation 7.0 eingeführten Installationsassistenten. Die Verwendung des Assistenten ist weiterhin die empfohlene Methode für Installationen ohne Skript und unterstützt Minimal- oder verteilte Bereitstellungen.
- Mit dieser Version von vRealize Automation wird eine konsolenbasierte Installation mit Skript eingeführt, die in Verbindung mit einer vorab konfigurierten Antwortdatei funktioniert.
- In dieser Version wird eine Befehlszeilenschnittstelle für Installationsaufgaben eingeführt, die Sie nach der anfänglichen Installation ausführen können, wie etwa das Hinzufügen einer weiteren vRealize Automation-Appliance zu Ihrer Bereitstellung für Hochverfügbarkeit.
- Mit dieser Version wird die Downloadseite des Installationsprogramms für Gast- und Software-Agenten geändert.

<https://vrealize-automation-appliance-FQDN/software/index.html>

Nach der Installation beginnen Sie mit der Verwendung von vRealize Automation, indem Sie die Umgebung anpassen und mindestens einen Mandanten konfigurieren. Damit wird der Zugriff auf Self-Service-Bereitstellung und Lebenszyklusverwaltung für Cloud-Dienste eingerichtet. Mit dem sicheren vRealize Automation-Webportal können Administratoren, Entwickler und Unternehmensbenutzer IT-Dienste anfordern und spezifische, auf ihren Rollen und Berechtigungen basierende Cloud- und IT-Ressourcen verwalten. Benutzer fordern Infrastruktur-, Anwendungs-, Desktop- und IT-Dienste über einen gemeinsamen Servicekatalog an.

Dieses Kapitel behandelt die folgenden Themen:

- „[Auswählen des Bereitstellungspfads](#)“, auf Seite 11
- „[vRealize Automation-Installationskomponenten](#)“, auf Seite 15

## Auswählen des Bereitstellungspfads

Je nach Ihren Bereitstellungsanforderungen können Sie vRealize Automation-Komponenten mit den Rainpole-Installationsszenario, dem Installationsassistenten oder über die Managementkonsole installieren und konfigurieren.

Wählen Sie eine Minimalinstallation aus, um eine Proof-of-Concept (PoC)- oder Entwicklungsumgebung mit einer grundlegenden Topologie bereitzustellen. Wählen Sie eine Unternehmensinstallation aus, um eine Produktionsumgebung mit der für Ihre Unternehmensanforderungen optimal geeigneten Topologie bereitzustellen.

**Tabelle 1-1.** Auswählen der Installationsmethode

Installationsmethode	Details
Installationsassistent	<p>Der Installationsassistent stellt für die meisten Bereitstellungen den schnellsten Installationspfad dar. Sie können sich für eine Minimal- oder Unternehmensbereitstellung entscheiden, um verteilte Komponenten mit oder ohne Lastausgleichsdienste zu unterstützen. Erfüllen Sie alle Voraussetzungen und überprüfen Sie sie, bevor Sie den Assistenten starten.</p> <p>Weitere Informationen finden Sie unter <a href="#">Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“</a>, auf Seite 19.</p>
Manuelle Installation	<p>Die Installation über die Managementkonsole wird für Minimal-, Hochverfügbarkeits- und verteilte Installationen ebenfalls unterstützt. Erfüllen Sie alle Voraussetzungen und überprüfen Sie sie, bevor Sie mit der Installation beginnen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“</a>, auf Seite 19.</p> <p><b>HINWEIS</b> Wenn Sie die Managementkonsole zum Starten oder Konfigurieren von Installationskomponenten verwenden, können Sie den Installationsassistenten nicht starten oder weiterhin verwenden.</p>
<i>Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario</i>	<p>Als ein vSphere-Administrator möchten Sie eine minimale vRealize Automation-Bereitstellung in Ihrer vorhandenen vSphere-Umgebung installieren. Sie verwenden den Installationsassistenten für die Installation von vRealize Automation und erstellen Katalogelemente für anfänglichen Inhalt, um eine Proof-of-Concept-Umgebung schnell und problemlos zu konfigurieren.</p> <p>Eine Proof-of-Concept-Bereitstellung ist für eine Produktionsumgebung ungeeignet. Nach Abschluss der Proof-of-Concept-Bereitstellung konfigurieren Sie diese als Entwicklungsumgebung, in der Sie und Ihr IT-Team Blueprints erstellen und testen. Sie können Blueprints und weitere Designelemente von Ihrer Entwicklungsumgebung in Ihre Produktionsumgebung exportieren.</p> <p>Informationen zum Starten dieses Szenarios finden Sie unter <i>Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario</i>.</p>

**Tabelle 1-2.** Auswählen des Bereitstellungstyps

Bereitstellungszweck	Empfohlener Bereitstellungstyp
Bereitstellung einer Proof-of-Concept (PoC)- oder Entwicklungsumgebung mit einer grundlegenden Topologie.	<p>Installieren einer Minimalbereitstellung.</p> <p>Sie stellen eine einzelne Instanz von vRealize Automation-Appliance bereit und installieren alle IaaS-Komponenten auf einer einzelnen Windows Server-Maschine. Sie können die Datenbanken auf derselben Windows-Maschine oder auf einer dedizierten SQL Server-Instanz installieren.</p>
Bereitstellung einer Produktionsumgebung mit der für Ihre Unternehmensanforderungen optimal geeigneten Topologie	<p>Installieren einer Unternehmensbereitstellung.</p> <p>Sie verteilen Komponenten auf mehrere Server.</p> <p>Optional können Sie Lastausgleichsdienste bereitstellen, um die Last auf Server zu verteilen und um Failover und Redundanz in einer High Availability-Umgebung zu ermöglichen.</p>

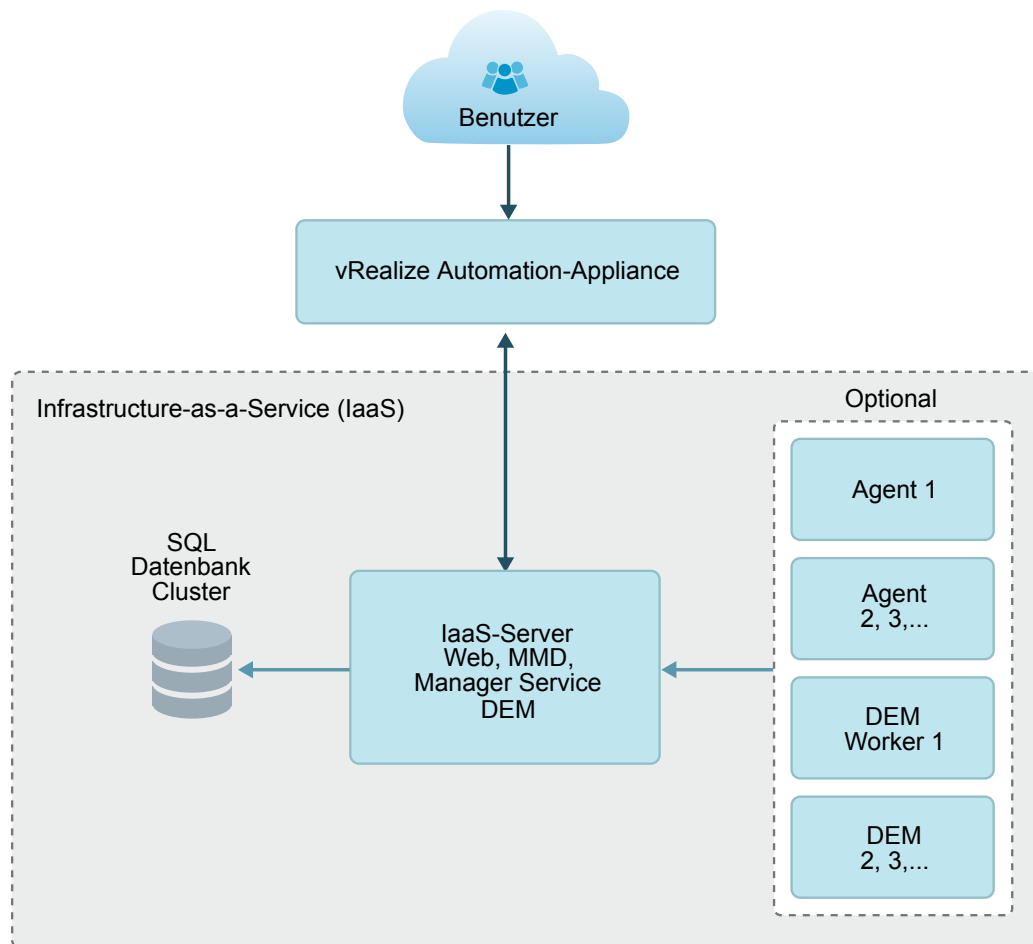
Informationen zu Skalierbarkeit und Hochverfügbarkeit finden Sie im Handbuch *vRealize Automation-Referenzarchitektur*.

## Überblick über Minimalbereitstellung

Um eine Minimalbereitstellung abzuschließen, installiert ein Systemadministrator die vRealize Automation-Appliance und die IaaS-Komponenten (Infrastructure as a Service).

- vRealize Automation-Appliance enthält die Schnittstelle der Webkonsole und Support für Funktionen für das einmalige Anmelden. Es wird als eine virtuelle Appliance installiert.
- IaaS (Infrastructure as a Service) wird auf einer Windows-Servermaschine installiert.
- IaaS verwendet eine SQL-Datenbank, die auf derselben Maschine wie IaaS oder auf dem eigenen Server installiert werden kann.

In der folgenden Abbildung sind die Beziehung und der Zweck von Komponenten einer Minimalinstallation dargestellt.



## Übersicht über die Unternehmensbereitstellung

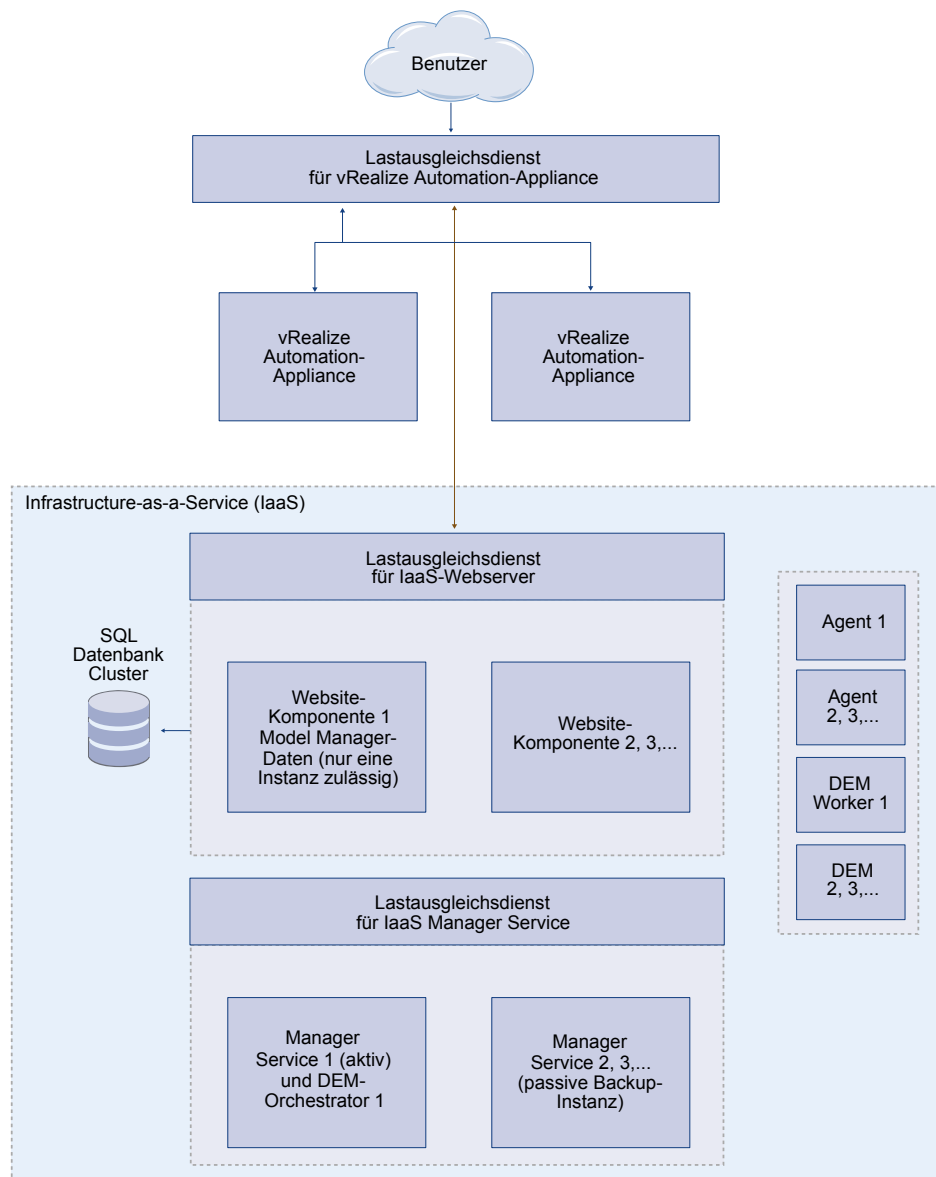
Der Systemadministrator kann mehrere Instanzen der vRealize Automation-Appliance und einzelne IaaS-Komponenten bereitstellen und installieren, um Skalierung, Redundanz, High Availability und Disaster Recovery zu unterstützen.

In einer typischen Architektur sind die IaaS-Komponenten auf mehrere Maschinen verteilt.

Für Hochverfügbarkeitsumgebungen verteilen Lastausgleichsdienste die Arbeitslast auf die Computing-Umgebung. Systemadministratoren konfigurieren Lastausgleichsdienste außerhalb des vRealize Automation-Frameworks.

In der folgenden Abbildung sind die Komponenten einer Unternehmensbereitstellung mit verteilten Komponenten, Redundanz und Lastausgleichsdiensten dargestellt.

**Abbildung 1-1.** Bereitstellungskonfiguration für Unternehmensinstallationen



## vRealize Automation -Installationskomponenten

Eine vRealize Automation-Installation enthält das Installieren und Konfigurieren von Funktionen für das einmalige Anmelden (Single Sign On, SSO), das Benutzerschnittstellenportal und IaaS-Komponenten (Infrastructure as a Service).

Eine Installation besteht aus den folgenden Komponenten.

- Die vRealize Automation-Appliance, die die Verwaltungskonsolle bereitstellt, verwaltet Single Sign-On-Funktionen (SSO) für die Autorisierung und Authentifizierung und enthält eine Instanz von vRealize Orchestrator.
- IaaS-Komponenten (Infrastructure as a Service), die auf virtuellen oder physischen Windows-Maschinen installiert sind und größtenteils auf der Registerkarte **Infrastruktur** der Konsole angezeigt werden.
- Eine Microsoft SQL Server-Datenbank, die bei der IaaS-Installation bereitgestellt wird.

### Die vRealize Automation -Appliance

Bei der vRealize Automation-Appliance handelt es sich um eine vorkonfigurierte virtuelle Linux-Appliance, die den vRealize Automation-Server enthält.

vRealize Automation wird als eine .ovf- oder .ova-Datei im Open Virtualization Format bereitgestellt. Sie stellen die virtuelle Appliance in einer vorhandenen virtualisierten Infrastruktur bereit.

Der Server enthält die vRealize Automation-Appliance-Produktkonsole, die ein einzelnes Portal für die Self-Service-Bereitstellung und Verwaltung von Cloud-Diensten sowie die Erstellung, Administration und Kontrolle bietet.

### Appliance-Datenbank

Während der Bereitstellung der virtuellen Appliances wird eine PostgreSQL-Appliance-Datenbank automatisch auf der ersten vRealize Automation-Appliance erstellt. Eine Replikatdatenbank kann in einer zweiten vRealize Automation-Appliance für Hochverfügbarkeit installiert werden.

### Management-Agents

Management-Agents sind eigenständige IaaS-Komponenten, die IaaS-Knoten bei vRealize Automation-Appliances registrieren, die Installation und das Management von IaaS-Komponenten automatisieren sowie Support- und Telemetrieinformationen erfassen.

Ein Management-Agent muss auf jeder Windows-Maschine installiert sein, die IaaS-Komponenten hostet.

### vRealize Automation Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) ermöglicht die schnelle Modellierung und Bereitstellung von Servern und Desktops in privaten, öffentlichen oder Hybrid-Cloud-Infrastrukturen.

Der Systemadministrator installiert IaaS-Komponenten auf einer Windows-Maschine. IaaS-Funktionen stehen auch auf der Registerkarte **Infrastruktur** in der Managementkonsole zur Verfügung. IaaS umfasst mehrere Komponenten, die Sie im Rahmen einer benutzerdefinierten Konfiguration installieren können, um die Anforderungen Ihrer Organisation zu erfüllen.

## IaaS-Website

Die IaaS-Website-Komponente stellt der vRealize Automation-Konsole die Funktionen für die Infrastrukturadministration und die Erstellung von Diensten zur Verfügung. Die Website-Komponente kommuniziert mit dem Manager Service, von welchem sie Updates vom Distributed Execution Manager (DEM), den Proxy-Agents und der Datenbank erhält.

## Model Manager

vRealize Automation-Modelle vereinfachen die Integration in externe Systeme und Datenbanken. Sie implementieren eine Geschäftslogik, die ein Distributed Execution Manager (DEM) verwendet.

Der Model Manager stellt Dienste und Dienstprogramme für Persistenz, Versionierung, Sichern und Verteilen von Modellelementen bereit. Er kommuniziert mit der Datenbank, den DEMs und der Konsolen-Website.

## Manager Service

Der 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.

Für Ihre IaaS-Bereitstellung ist es erforderlich, dass der Manager Service nur auf einer Windows-Maschine aktiv ausgeführt wird. Für Backups oder Hochverfügbarkeit können Sie zusätzliche Windows-Maschinen bereitstellen, auf denen Sie den Manager Service manuell starten, falls der aktive Dienst beendet wird.

---

**WICHTIG** Die gleichzeitige Ausführung eines aktiven Manager Service auf mehreren IaaS-Windows-Servern hat zur Folge, dass vRealize Automation nicht verwendet werden kann.

---

Der Manager Service kommuniziert mit der IaaS-Website über den Model Manager und muss unter einem Domänenkonto mit Administratorrechten auf allen IaaS-Windows-Maschinen ausgeführt werden.

## IaaS-Datenbank

Die IaaS-Komponente von vRealize Automation verwendet eine Microsoft SQL Server-Datenbank, um Informationen zu den verwalteten Maschinen und zu den eigenen Elementen und Richtlinien zu warten. In der Regel wird die Datenbank während der Installation automatisch erstellt. Ein Systemadministrator kann jedoch die Datenbank auch separat erstellen.

## Distributed Execution Manager

Ein Distributed Execution Manager (DEM) führt die Geschäftslogik von benutzerdefinierten Modellen aus und interagiert bei Bedarf mit der Datenbank und mit externen Datenbanken und Systemen.

Jede DEM-Instanz fungiert entweder als Worker- oder Orchestrator-Rolle. Die Worker-Rolle ist für die Ausführung von Workflows zuständig. Die Orchestrator-Rolle ist für die Überwachung der DEM-Worker-Instanzen, die Vorverarbeitung von auszuführenden Workflows und die Planung von Workflows zuständig.

Der DEM-Orchestrator führt die folgenden Aufgaben aus.

- Überwacht den Status von DEM-Worker-Instanzen, Wenn eine Worker-Instanz beendet wird oder die Verbindung zum Model Manager getrennt wird, stellt er außerdem sicher, dass die zugehörigen Workflows wieder in die Warteschlange gestellt werden, damit sie von einem anderen DEM-Worker abgerufen werden.
- Verwaltet geplante Workflows durch das Erstellen neuer Workflowinstanzen zum geplanten Zeitpunkt.
- Stellt sicher, dass jeweils nur eine Instanz eines bestimmten geplanten Workflows ausgeführt wird.



- Verarbeitet Workflows vor der Ausführung, einschließlich der Überprüfung der Vorbedingungen für Workflows, die bei der Implementierung der RunOnceOnly-Funktion verwendet werden, sowie der Erstellung des Workflowausführungsverlaufs.

Eine DEM-Orchestrator-Instanz wird als aktiver Orchestrator festgelegt, der diese Aufgaben ausführt. Der DEM-Orchestrator spielt eine wichtige Rolle beim Ausführen von Workflows, weshalb Sie aus Redundanzgründen mindestens eine zusätzliche Orchestrator-Instanz auf einer separaten Maschine installieren sollten. Der Orchestrator wird automatisch auf der Maschine installiert, auf der auch der Manager Service ausgeführt wird. Der zusätzliche DEM-Orchestrator überwacht den Status des aktiven Orchestrators, damit er übernehmen kann, wenn der aktive Orchestrator in den Offlinemodus wechselt.

## **vRealize Automation -Agents**

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

Im Allgemeinen installieren Sie den vSphere-Agent als Teil einer Bereitstellung. Gemäß den Anforderungen Ihrer Site können Sie weitere Agents installieren.

### **Integrations-Agents**

Virtual Desktop Integration (VDI) PowerShell-Agents ermöglichen vRealize Automation die Integration in externe virtuelle Desktopsysteme. Derzeit können virtuelle Maschinen, die von vRealize Automation bereitgestellt werden, mit XenDesktop auf einem Citrix Desktop Delivery Controller (DDC) registriert werden, und die Besitzer können über vRealize Automation auf die XenDesktop-Webschnittstelle zugreifen.

External Provisioning Integration (EPI) PowerShell-Agents ermöglichen vRealize Automation die Integration in externe 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.

VDI- und EPI-Agents erfordern Administratorzugriff auf die externen Systeme, mit denen sie interagieren.

### **Virtualisierungs-Proxy-Agents**

Die virtuellen Maschinen, die von vRealize Automation verwaltet werden, werden auf Virtualisierungshosts erstellt. vRealize Automation sendet mithilfe von Virtualisierungs-Proxy-Agents Befehle und erfasst Daten von vSphere ESX Server, XenServer und Hyper-V-Virtualisierungshosts und den auf diesen bereitgestellten virtuellen Maschinen. Ein Proxy-Agent weist die folgenden Merkmale auf.

- Erfordert in der Regel Administratorzugriff auf die von diesem Agent verwaltete Virtualisierungsplattform
- Kommuniziert mit dem Manager Service
- Wird separat mit einer eigenen Konfigurationsdatei installiert

### **Windows-Verwaltungsinstrumentations-Agent (WMI)**

Der vRealize Automation Windows-Verwaltungsinstrumentations-Agent (WMI) optimiert die Überwachung und Kontrolle der Systeminformationen und ermöglicht die zentrale Verwaltung von Remote-Servern. Dieser Agent ermöglicht außerdem die Erfassung von Daten auf Windows-Maschinen, die von vRealize Automation verwaltet werden.



# Vorbereitung für die Installation von vRealize Automation

# 2

Systemadministratoren installieren vRealize Automation in ihre vorhandenen Virtualisierungsumgebungen. Bereiten Sie die Bereitstellungsumgebung gemäß den Systemanforderungen vor, bevor Sie eine Installation beginnen.

Dieses Kapitel behandelt die folgenden Themen:

- „Hostnamen und IP-Adressen“, auf Seite 19
- „Anforderungen an die Hardware und an virtuelle Maschinen“, auf Seite 20
- „Überlegungen zum Browser“, auf Seite 20
- „Überlegungen zum Kennwort“, auf Seite 21
- „Anforderungen an Windows Server“, auf Seite 21
- „vRealize Automation-Portanforderungen“, auf Seite 26
- „Für die Installation erforderliche Benutzerkonten und Anmeldedaten“, auf Seite 29
- „Sicherheit“, auf Seite 30
- „Uhrzeitsynchronisierung“, auf Seite 32

## Hostnamen und IP-Adressen

vRealize Automation verlangt, dass bei der Benennung von Hostnamen in Ihrer Installation bestimmte Voraussetzungen erfüllt sein müssen.

- Alle vRealize Automation-Maschinen in Ihrer Installation müssen sich gegenseitig über den vollqualifizierten Domännennamen (FQDN) auflösen können.

Geben Sie bei der Installation stets den FQDN ein, wenn Sie eine Maschine identifizieren oder auswählen. Geben Sie keine IP-Adressen 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 vorab, sodass die Namen von vRealize Automation-Maschinen mit Buchstaben (a-z) oder Ziffern (0-9) beginnen und enden und nur Buchstaben, Ziffern und 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](http://www.ietf.org).

- Behalten Sie die für vRealize Automation-Systeme geplanten Hostnamen und FQDNs möglichst bei. Wird ein Hostname nach der Installation geändert, kann vRealize Automation nicht mehr genutzt werden.
- Es empfiehlt sich, statische IP-Adressen für alle vRealize Automation-Appliance-Instanzen 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.

## Anforderungen an die Hardware und an virtuelle Maschinen

Die Bereitstellung muss über ein Minimum an Systemressourcen verfügen, um virtuelle Appliances installieren zu können, und stellt Mindestanforderungen an die Hardware, um IaaS-Komponenten auf dem Windows-Server installieren zu können.

Informationen zu den Betriebssystem- und allgemeinen Umgebungsanforderungen, einschließlich Informationen zu unterstützten Browsern und Betriebssystemen, finden Sie in der *Übersicht über die Unterstützung von vRealize Automation*.

In der Tabelle zu den Hardwareanforderungen werden die Mindestanforderungen an die Konfiguration für die Bereitstellung virtueller Appliances und die Installation von IaaS-Komponenten angezeigt. Bei Appliances handelt es sich um vorkonfigurierte virtuelle Maschinen, die Sie zu Ihrer vCenter Server- oder ESXi-Bestandsliste hinzufügen. IaaS-Komponenten werden auf physischen oder virtuellen Windows 2008 R2 SP1- oder Windows 2012 R2-Servern installiert.

Ein Active Directory wird als klein betrachtet, wenn nicht mehr als 25.000 Benutzer in der OU (Organisationseinheit, Organization Unit) bei der Identitätsquellenkonfiguration synchronisiert werden müssen. Ein Active Directory wird als groß betrachtet, wenn sich mehr als 25.000 Benutzer in der OU befinden.

**Tabelle 2-1.** Hardwareanforderungen

vRealize Automation-Appliance für kleine Active Directories	vRealize Automation-Appliance für große Active Directories	IaaS-Komponenten (Windows-Server).
<ul style="list-style-type: none"> <li>■ 4 CPUs</li> <li>■ 18 GB Arbeitsspeicher</li> <li>■ 60 GB Festplattenspeicher</li> </ul>	<ul style="list-style-type: none"> <li>■ 4 CPUs</li> <li>■ 22 GB Arbeitsspeicher</li> <li>■ 60 GB Festplattenspeicher</li> </ul>	<ul style="list-style-type: none"> <li>■ 2 CPUs</li> <li>■ 8 GB Arbeitsspeicher</li> <li>■ 30 GB Festplattenspeicher</li> </ul> <p>Zusätzliche Ressourcen sind erforderlich, wenn Sie auf einem Windows-Host einen SQL-Server hinzufügen.</p>

## Überlegungen zum Browser

Für die Verwendung eines Browsers mit vRealize Automation gelten einige Einschränkungen.

- 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.

Informationen zu den Betriebssystem- und allgemeinen Umgebungsanforderungen, einschließlich Informationen zu unterstützten Browsern und Betriebssystemen, finden Sie in der *Übersicht über die Unterstützung von vRealize Automation*.

## Überlegungen zum Kennwort

Es gelten bestimmte Zeicheneinschränkungen für einige Kennwörter.

Das VMware vRealize™ Automation-Administratorkennwort darf kein angehängtes =-Zeichen enthalten. Derartige Kennwörter werden bei der Zuweisung akzeptiert, führen aber zu Fehlern, wenn Sie Vorgänge wie beispielsweise das Speichern von Endpoints durchführen.

## Anforderungen an Windows Server

Die virtuelle oder physische Windows-Maschine, die die IaaS-Komponenten hostet, muss die Konfigurationsanforderungen für die IaaS-Datenbank, die IaaS-Server-Komponenten, den IaaS Manager Service und die Distributed Execution Manager erfüllen.

Der Installationsassistent führt eine vRealize Automation-Voraussetzungsprüfung auf allen IaaS-Windows-Servern aus, um sicherzustellen, dass sie die Konfigurationsanforderungen für die Installation erfüllen. Prüfen Sie zusätzlich zur Voraussetzungsprüfung die folgenden Voraussetzungen separat.

- Es wird empfohlen, alle IaaS-Windows-Server in derselben Domäne zu platzieren.
- Erstellen oder bestimmen Sie ein für die Installation zu verwendendes Domänenkonto. Dies sollte ein Konto sein, das auf allen IaaS-Windows-Servern über Administratorrechte verfügt.

## IaaS -Datenbankserveranforderungen

Der Windows-Server, der die vRealize Automation IaaS SQL Server-Datenbank hostet, muss bestimmte Voraussetzungen erfüllen.

Die Anforderungen gelten unabhängig davon, ob Sie den Installationsassistenten oder das ältere Installationsprogramm `setup_vrealize-automation-appliance-URL.exe` ausführen und die Datenbankrolle für die Installation auswählen. Die Anforderungen gelten auch, wenn Sie separat eine leere SQL Server-Datenbank für die Verwendung mit IaaS erstellen.

- Verwenden Sie eine unterstützte Version von SQL Server von der *Übersicht über die Unterstützung von vRealize Automation*.
- Aktivieren Sie das TCP/IP-Protokoll für SQL Server.
- Aktivieren Sie den DTC-Dienst (Distributed Transaction Coordinator) auf allen IaaS-Windows-Servern und auf der Maschine, die SQL Server hostet. 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](#)“, auf Seite 149.

---

Weitere Informationen zur DTC-Aktivierung finden Sie im [VMware Knowledgebase-Artikel 2038943](#).

- Geben Sie Ports zwischen allen IaaS-Windows-Servern und der Maschine frei, die SQL Server hostet. Siehe „[vRealize Automation-Portanforderungen](#)“, auf Seite 26.

Alternativ können Sie Firewalls zwischen IaaS-Windows-Servern und SQL Server deaktivieren, sofern die Richtlinien der Site dies zulassen.

- Diese Version von vRealize Automation unterstützt nicht den Kompatibilitätsmodus 130 für SQL Server 2016. Wenn Sie separat eine leere SQL Server 2016-Datenbank für die Verwendung mit IaaS erstellen, verwenden Sie den Kompatibilitätsmodus 100 oder 120.

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

- AlwaysOn-Verfügbarkeitsgruppe (AlwaysOn Availability Group, AAG) wird nur für SQL Server 2016 unterstützt.

## Anforderungen an den IaaS-Webdienst und den Model Manager-Server

Ihre Umgebung muss Voraussetzungen bezüglich Software und Konfiguration erfüllen, um die Installation der IaaS-Serverkomponenten zu unterstützen.

### Umgebung und Datenbankanforderungen für IaaS

Ihre Hostkonfiguration und MS SQL-Datenbank müssen die folgenden Anforderungen erfüllen.

**Tabelle 2-2.** IaaS-Anforderungen

Bereich	Anforderungen
Hostkonfiguration	<p>Die folgenden Komponenten müssen auf dem Host installiert werden, bevor Sie IaaS installieren können:</p> <ul style="list-style-type: none"> <li>■ Microsoft .NET Framework 4.5.2 oder höher.</li> <li>■ Microsoft PowerShell 2.0 (im Lieferumfang von Windows Server 2008 R2 SP1 und höher enthalten) oder Microsoft PowerShell 3.0 unter Windows Server 2012 R2.</li> <li>■ Microsoft Internetinformationsdienste 7.5.</li> <li>■ Auf der Maschine, auf der die primäre Webkomponente ausgeführt wird, muss Java installiert sein, um die Bereitstellung der MS SQL-Datenbank bei der Installation zu unterstützen.</li> </ul>
Microsoft SQL-Datenbankanforderungen	<p>Die SQL-Datenbank kann sich auf einem der IaaS-Windows-Server oder auf einem separaten Host befinden.</p> <p>Falls sich die SQL-Datenbank auf einem der IaaS-Windows-Server befindet, konfigurieren Sie die folgenden Java-Anforderungen.</p> <ul style="list-style-type: none"> <li>■ Installieren Sie Java 1.8 (64 Bit) oder höher. Verwenden Sie nicht die 32-Bit-Version.</li> <li>■ Legen Sie die Umgebungsvariable JAVA_HOME auf den Java-Installationsordner fest.</li> <li>■ Überprüfen Sie, ob die Datei „%JAVA_HOME%\bin\java.exe“ verfügbar ist.</li> </ul>

### Anforderungen an Microsoft Internetinformationsdienste

Konfigurieren Sie Internetinformationsdienste (IIS) entsprechend der nachfolgenden Anforderungen.

Neben den Konfigurationseinstellungen sollten Sie darauf achten, keine zusätzlichen Websites in IIS auf dem IaaS-Webserverhost zu hosten. 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 2-3.** Erforderliche Konfiguration für Microsoft Internetinformationsdienste

IIS-Komponente	Einstellung
Installierte Internetinformationsdienste (IIS)-Module	<ul style="list-style-type: none"> <li>■ WindowsAuthentication</li> <li>■ StaticContent</li> <li>■ DefaultDocument</li> <li>■ ASPNET 4.5</li> <li>■ ISAPIExtensions</li> <li>■ ISAPIFilter</li> </ul>
IIS-Authentifizierungseinstellungen	<ul style="list-style-type: none"> <li>■ Windows-Authentifizierung aktiviert</li> <li>■ Anonyme Authentifizierung deaktiviert</li> <li>■ Anbietershandlung aktiviert</li> <li>■ NTLM-Anbieter aktiviert</li> <li>■ Kernelmodus der Windows-Authentifizierung aktiviert</li> <li>■ Erweiterter Schutz der Windows-Authentifizierung deaktiviert</li> <li>■ Für Zertifikate, die SHA512 verwenden, muss TLS1.2 auf Windows 2012- oder Windows 2012 R2-Servern deaktiviert werden.</li> </ul>
IIS-Rollen des Windows-Prozessaktivierungsdiensts	<ul style="list-style-type: none"> <li>■ ConfigurationApi</li> <li>■ NetEnvironment</li> <li>■ ProcessModel</li> <li>■ WcfActivation (nur Windows 2008)</li> <li>■ HttpActivation</li> <li>■ NonHttpActivation</li> </ul>

## IaaS Manager Service

Ihre Umgebung muss einige allgemeine Anforderungen erfüllen, die die Installation des IaaS Manager Service unterstützen.

- Microsoft .NET Framework 4.5.2 ist installiert.
- Microsoft PowerShell 2.0, 3.0 oder 4.0. Für manche vRealize Automation-Upgrades oder -Migrationen müssen Sie zusätzlich zur aktuell verwendeten PowerShell-Version möglicherweise eine ältere oder neuere PowerShell-Version installieren.
- SecondaryLogOnService wird ausgeführt.
- Es dürfen keine Firewalls zwischen DEM-Host und Windows Server vorhanden sein. Portinformationen finden Sie unter „[vRealize Automation-Portanforderungen](#)“, auf Seite 26.
- IIS ist installiert und konfiguriert.

## Anforderungen an den Distributed Execution Manager

Ihre Umgebung muss einige allgemeine Anforderungen erfüllen, die die Installation von Distributed Execution Manager (DEM)-Instanzen unterstützen.

- Microsoft .NET Framework 4.5.2 ist installiert.
- Microsoft PowerShell 2.0, 3.0 oder 4.0. Für manche vRealize Automation-Upgrades oder -Migrationen müssen Sie zusätzlich zur aktuell verwendeten PowerShell-Version möglicherweise eine ältere oder neuere PowerShell-Version installieren.
- SecondaryLogOnService wird ausgeführt.

- Keine Firewalls zwischen DEM-Host und dem Windows-Server, oder geöffnete Ports wie unter „[vRealize Automation-Portanforderungen](#)“, auf Seite 26 beschrieben.

Für Server, die DEM-Worker-Instanzen hosten, gelten in Abhängigkeit von den Bereitstellungsressourcen, mit denen sie interagieren, möglicherweise zusätzliche Anforderungen.

## Anforderungen für Amazon Web Services EC2

Ein vRealize Automation IaaS-Windows-Server kommuniziert mit und sammelt Daten von einem Amazon-EC2-Konto.

Wenn Sie Amazon Web Services (AWS) für die Bereitstellung verwenden, müssen die IaaS-Windows-Server, die DEM-Workers hosten, folgende Anforderungen erfüllen:

- DEM-Worker-Hosts müssen über Internetzugriff verfügen.
- Wenn sich die DEM-Worker-Hosts hinter einer Firewall befinden, 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 die DEM-Worker-Hosts über einen Proxy-Server ins Internet gelangen, muss der DEM-Dienst unter Anmeldedaten ausgeführt werden, mit denen eine Authentifizierung beim Proxy-Server erfolgen kann.



## Anforderungen für OpenStack und PowerVC

Die Maschinen, auf denen Sie Ihre DEMs installieren, müssen bestimmte Anforderungen erfüllen, um mit Ihrer OpenStack- oder PowerVC-Instanz zu kommunizieren oder Daten dafür zu erfassen.

**Tabelle 2-4.** DEM-Hostanforderungen

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> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</p>
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> <p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</p>
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>

## Anforderungen für Red Hat Enterprise Virtualization KVM (RHEV)

Wenn Sie Red Hat Enterprise Virtualization für die Bereitstellung verwenden, kommuniziert der IaaS-Windows-Server mit diesem Konto und erfasst Daten aus diesem Konto.

Ihre Umgebung muss die folgenden Anforderungen für Red Hat Enterprise erfüllen.

- Jede KVM (RHEV)-Umgebung muss mit der Domäne verknüpft werden, die den IaaS-Server enthält.
- Die Anmeldedaten, die für die Verwaltung des Endpoints verwendet werden, welcher eine KVM (RHEV)-Umgebung darstellt, müssen über Administratorberechtigungen in der RHEV-Umgebung verfügen. Diese Anmeldedaten müssen auch über ausreichende Berechtigungen zum Erstellen von Objekten auf den Hosts innerhalb der Umgebung verfügen.

## SCVMM-Anforderungen

Jeder DEM Worker, der für die Verwaltung von virtuellen Maschinen über SCVMM verwendet wurde, muss auf einem Host installiert werden, auf dem die SCVMM-Konsole bereits installiert ist.

Zudem müssen die folgenden Anforderungen erfüllt sein:

- Der DEM muss Zugriff auf das SCVMM-PowerShell-Modul haben, das mit der Konsole installiert ist.

- 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:

```
help about_signing
help Set-ExecutionPolicy
```

- Wenn sich keine DEM-Workers innerhalb der Instanz auf Computing-Ressourcen befinden, die diese Anforderungen erfüllen, müssen „Qualifikationen“ verwendet werden, um alle SCVMM-bezogenen Workflows denjenigen Computing-Ressourcen zuzuweisen, die die Anforderungen erfüllen.

Die folgenden zusätzlichen Anforderungen gelten für SCVMM.

- Sie müssen die SCVMM-Konsole installieren, bevor Sie die DEM-Workers installieren, die SCVMM-Arbeitselemente in Anspruch nehmen.

Wenn Sie die DEM Worker vor der SCVMM-Konsole installieren, werden Protokollfehler ähnlich dem folgenden 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 dies zu beheben, stellen Sie sicher, dass die SCVMM-Konsole installiert ist, und starten Sie den DEM Worker-Dienst neu.

- Jede SCVMM-Instanz muss mit der Domäne verbunden sein, die den Server enthält.
- Die Anmeldedaten, die zur Verwaltung des die SCVMM-Instanz darstellenden Endpoints verwendet werden, müssen über Administratorrechte auf dem SCVMM-Server verfügen. Diese Anmeldedaten müssen auch auf den Hyper-V Servern innerhalb der Instanz über Administratorrechte 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 die Bereitstellung von Maschinen auf einer SCVMM-Computing-Ressource durchführen zu können, muss ein Benutzer zu mindestens einer Sicherheitsrolle innerhalb der SCVMM-Instanz hinzugefügt werden.

## vRealize Automation -Portanforderungen

vRealize Automation verwendet festgelegte Ports für die Kommunikation und den Datenzugriff.

Obwohl vRealize Automation nur Port 443 für die Kommunikation verwendet, sind möglicherweise andere Ports auf dem System geöffnet. Da geöffnete, ungesicherte Ports Sicherheitsrisiken darstellen können, stellen Sie sicher, dass nur die Ports geöffnet sind, die von Ihren Geschäftsanwendungen benötigt werden.

## vRealize Automation -Appliance

Die folgenden Ports werden von der vRealize Automation-Appliance verwendet.

**Tabelle 2-5.** Eingehende Ports für die vRealize Automation-Appliance

Port	Protokoll	Anmerkungen
22	TCP	Optional. Zugriff auf SSH-Sitzungen.
80	TCP	Optional. Leitet weiter zu 443.

**Tabelle 2-5.** Eingehende Ports für die vRealize Automation-Appliance (Fortsetzung)

Port	Protokoll	Anmerkungen
111	TCP, UDP	RPC.
443	TCP	Zugriff auf die vRealize Automation-Konsole und API-Aufrufe.
443	TCP	Zugriff für Maschinen zum Herunterladen des Gast-Agents und des Software-Bootstrap-Agents.
5480	TCP	Zugriff auf die Web-Verwaltungsschnittstelle der virtuellen Appliance.
5480	TCP	Verwendet vom Management-Agent.
5488, 5489	TCP	Intern von der vRealize Automation-Appliance für Updates verwendet.
4369, 25672,5671,5672	TCP	RabbitMQ-Messaging.
8230, 8280, 8281	TCP	Interne vRealize Orchestrator-Instanz.
8444	TCP	Konsolenproxykommunikation für vSphere VMware Remote Console-Verbindungen.

**Tabelle 2-6.** Ausgehende Ports für die vRealize Automation -Appliance

Port	Protokoll	Anmerkungen
25, 587	TCP, UDP	SMTP für das Senden von ausgehenden Benachrichtigungs-E-Mails.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Optional. Für das Abrufen von Softwareaktualisierungen. Aktualisierungen können separat heruntergeladen und angewendet werden.
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.
443	TCP	Kommunikation mit IaaS Manager Service und Infrastruktur-Endpoint-Hosts über HTTPS
443	TCP	Kommunikation mit dem Software-Bootstrap-Agent über HTTPS.
902	TCP	Kopiervorgänge für ESXi-Netzwerkdatei und VMware Remote Console-Verbindungen.
5050	TCP	Optional. Für die Kommunikation mit vRealize Business.
5432	TCP, UDP	Optional. Für die Kommunikation mit einer Appliance-Datenbank.
8281	TCP	Optional. Für die Kommunikation mit einer externen vRealize Orchestrator-Instanz.

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.

## Infrastructure-as-a-Service

Die Ports in den Tabellen „Eingehende Ports für Infrastructure-as-a-Service-Komponenten“ und für „Ausgehende Ports für Infrastructure-as-a-Service-Komponenten“ müssen für die Verwendung durch den IaaS-Windows-Server verfügbar sein.

**Tabelle 2-7.** Eingehende Ports für Infrastructure-as-a-Service-Komponenten

Komponente	Port	Protokoll	Anmerkungen
Manager Service	443	TCP	Kommunikation mit IaaS-Komponenten und vRealize Automation-Appliance über HTTPS.
vRealize Automation-Appliance	443	TCP	Kommunikation mit IaaS-Komponenten und vRealize Automation-Appliance über HTTPS.
Infrastruktur-Endpoint-Hosts	443	TCP	Kommunikation mit IaaS-Komponenten und 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.
SQL Server-Instanz	1433	TCP	MSSQL.

**Tabelle 2-8.** Ausgehende Ports für Infrastructure-as-a-Service-Komponenten

Komponente	Port	Protokoll	Anmerkungen
Alle	53	TCP, UDP	DNS.
Alle	67, 68, 546, 547	TCP, UDP	DHCP.
Alle	123	TCP, UDP	Optional. NTP.
Manager Service	443	TCP	Kommunikation mit vRealize Automation-Appliance über HTTPS.
Website	443	TCP	Kommunikation mit Manager Service über HTTPS. Kommunikation mit vCenter Server über HTTPS.
Distributed Execution Manager	443	TCP	Kommunikation mit Manager Service über HTTPS.
Proxy-Agents	443	TCP	Kommunikation mit Manager Service und Infrastruktur-Endpoint-Hosts über HTTPS.
Management-Agent	443	TCP	Kommunikation mit der vRealize Automation-Appliance.
Gast-Agent Software-Bootstrap-Agent	443	TCP	Kommunikation mit Manager Service über HTTPS.
Manager Service Website	1433	TCP	MSSQL.
Alle	5480	TCP	Kommunikation mit der vRealize Automation-Appliance.

## Microsoft Distributed Transaction Coordinator-Dienst

Zusätzlich zu der Überprüfung, dass die in den vorhergehenden Tabellen aufgelisteten Ports kostenlos für die Verwendung sind, müssen Sie die Kommunikation für den Microsoft Distributed Transaction Coordinator-Dienst (MS DTC) zwischen allen Servern in der Bereitstellung aktivieren. MS DTC erfordert die Verwendung von Port 135 über TCP und einen zufälligen Port zwischen 1024 und 65535.

Die Voraussetzungsprüfung überprüft, ob MS DTC ausgeführt wird und ob die erforderlichen Ports geöffnet sind.

## Für die Installation erforderliche Benutzerkonten und Anmeldedaten

Sie müssen sicherstellen, dass Sie über die Rollen und Anmeldedaten verfügen, um die Installation der vRealize Automation-Komponenten durchführen zu können.

### vCenter-Dienstkonto

Für die Verwendung eines vSphere-Endpoints benötigen Sie ein Domänenkonto oder ein lokales Konto, das über die entsprechenden Berechtigungen in vCenter verfügt, die den Benutzern zugewiesen wurden.

### Installation der virtuellen Appliance

Zur Bereitstellung der vRealize Automation-Appliance müssen Sie auf der Bereitstellungsplattform über die entsprechenden Rechte (z. B. vSphere-Administratoranmeldedaten) verfügen.

Während des Bereitstellungsvorgangs legen Sie das Kennwort für das Administratorkonto der virtuellen Appliance fest. Dieses Konto ermöglicht den Zugriff auf die vRealize Automation-Appliance-Managementkonsole, über die Sie die virtuellen Appliances konfigurieren und verwalten.

### IaaS-Installation

Fügen Sie vor der Installation der IaaS-Komponenten denjenigen Benutzer zur Administratorgruppe auf dem Installations-Host hinzu, mit dem die IaaS-Installationsprogramme ausgeführt werden sollen.

### IaaS-Datenbankanmeldedaten

Sie können die Datenbank während der Produktinstallation oder manuell in SQL Server erstellen.

Wenn Sie eine MS SQL-Datenbank über vRealize Automation mithilfe des Installationsassistenten oder der Managementkonsole erstellen oder auffüllen, gelten die folgenden Anforderungen:

- Bei Verwendung der Option **Windows-Authentifizierung verwenden** muss die **sysadmin**-Rolle in SQL Server dem Benutzer erteilt werden, der den Management-Agent auf dem primären IaaS-Webserver ausführt, um die Datenbank zu erstellen und deren Größe zu ändern.
- Wenn Sie **Windows-Authentifizierung verwenden** nicht auswählen, muss die **sysadmin**-Rolle in SQL Server auch dem Benutzer erteilt werden, der den Management-Agent auf dem primären IaaS-Webserver ausführt. Die Anmeldedaten werden zur Laufzeit verwendet.
- Wenn Sie eine im Voraus erstellte Datenbank über vRealize Automation auffüllen, müssen die angegebenen Benutzeranmeldedaten (entweder der aktuelle Windows-Benutzer oder der angegebene SQL-Benutzer) nur **dbo**-Berechtigungen für die IaaS-Datenbank enthalten.

---

**HINWEIS** vRealize Automation-Benutzer müssen auch über die entsprechenden Berechtigungen bei der Windows-Authentifizierung verfügen, damit die Anmeldung bei und Verwendung von vRealize Automation möglich ist.

---

### Benutzeranmeldedaten für IaaS-Dienst

IaaS installiert mehrere Windows-Dienste, die einen einzelnen Dienst-Benutzer gemeinsam nutzen.

Die folgenden Anforderung gelten für den Dienst-Benutzer für IaaS-Dienste:

- Der Benutzer muss ein Domänenbenutzer sein.
- Der Benutzer muss auf allen Hosts, auf denen die Komponente des Manager Service oder der Website installiert ist, über lokale Administratorrechte verfügen. Führen Sie keine Arbeitsgruppen-Installation durch.

- Der Benutzer wird mit **Als Dienst anmelden**-Berechtigungen konfiguriert. Durch diese Berechtigung wird sichergestellt, dass der Manager Service startet und Protokolldateien generiert.
- Der Benutzer muss für die IaaS-Datenbank über **dbo**-Berechtigungen verfügen. Wenn Sie das Installationsprogramm zum Erstellen der Datenbank verwenden, stellen Sie sicher, dass die Dienst-Benutzeranmeldung zu SQL Server hinzugefügt wird, bevor das Installationsprogramm ausgeführt wird. Das Installationsprogramm gewährt dem Dienst-Benutzer nach dem Erstellen der Datenbank **dbo**-Berechtigungen.
- Das Installationsprogramm wird unter dem Konto ausgeführt, mit dem der Management-Agent auf dem primären Webserver ausgeführt wird. Wenn Sie das Installationsprogramm zum Erstellen einer MS SQL-Datenbank während der Installation verwenden möchten, muss die **sysadmin**-Rolle in MS SQL aktiviert sein. Dies ist nicht erforderlich, wenn Sie eine vorgefertigte leere Datenbank verwenden.
- Das Domänenbenutzerkonto, das für den Model Manager-Webservice als IIS-Anwendungspool-Identität verwendet werden soll, wird mit **Als Batch-Auftrag anmelden**-Berechtigungen konfiguriert.

## Spezifikationen für Model Manager-Server

Geben Sie den Namen des Model Manager-Servers als vollqualifizierten Domännennamen (FQDN) an. Verwenden Sie für die Angabe des Servers keine IP-Adresse.

## Sicherheit

vRealize Automation verwendet SSL, um eine sichere Kommunikation zwischen Komponenten sicherzustellen. Passphrasen werden für sichere Datenbankspeicher verwendet.

Weitere Informationen finden Sie unter „[Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung](#)“, auf Seite 67.

## 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, Support und Anforderungen im Hinblick auf die Vertrauenswürdigkeit von Zertifikaten finden Sie im [VMware Knowledgebase-Artikel 2106583](#).

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 2-9.** 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.

## Extrahieren von Zertifikaten und privaten Schlüsseln

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

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

**Tabelle 2-10.** Beispielzertifikatwerte und -befehle (openssl)

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

## Sicherheitskennwortsatz

vRealize Automation verwendet für die Sicherheit von Datenbanken Sicherheitskennwortsätze. Bei einem Kennwortsatz handelt es sich um eine Reihe von Wörtern, die zur Erstellung eines Satzes verwendet werden, welcher den Verschlüsselungsschlüssel zum Schutz der ruhenden Daten in der Datenbank generiert.

Befolgen Sie bei der ersten Erstellung eines Sicherheitskennwortsatzes die folgenden Richtlinien.

- Verwenden Sie über die gesamte Installation hinweg denselben Sicherheitskennwortsatz. Dadurch stellen Sie sicher, dass jede Komponente über denselben Verschlüsselungsschlüssel verfügt.
- Erstellen Sie einen Satz mit einer Länge von mehr als acht Zeichen.
- Verwenden Sie Großbuchstaben, Kleinbuchstaben, numerische Zeichen sowie Symbole.

- Merken Sie sich den Kennwortsatz oder bewahren Sie ihn an einem sicheren Ort auf. Der Kennwortsatz wird benötigt, um Datenbankinformationen bei einem Systemfehler wiederherzustellen oder um Komponenten nach der Erstinstallation hinzuzufügen. Ohne den Kennwortsatz können Sie keine erfolgreiche Wiederherstellung durchführen.

## Drittanbietersoftware

Einige Komponenten von vRealize Automation hängen von Drittanbietersoftware ab, wie z. B. Microsoft Windows und SQL Server. Stellen Sie zum Schutz vor Sicherheitslücken bei Drittanbieterprodukten sicher, dass Ihre Software auf dem aktuellen Stand ist und Sie immer die neuesten Patches des Anbieters einlesen.

## Uhrzeitsynchronisierung

Ein Systemadministrator muss als Teil der vRealize Automation-Installation eine genaue Zeiterfassung einrichten.

Die Installation schlägt fehl, wenn die Uhrzeitsynchronisierung nicht ordnungsgemäß eingerichtet wurde.

Die Zeiterfassung muss in allen vRealize Automation-Appliance und Windows-Servern konsistent und synchronisiert sein. Sie können die Konsistenz sicherstellen, indem Sie für jede Komponente dieselbe Zeiterfassungsmethode verwenden.

Für virtuelle Maschinen können Sie die folgenden Methoden verwenden:

- Konfiguration mit Network Time Protocol (direkt).
- Konfiguration mit Network Time Protocol durch ESXi mit VMware Tools. NTP muss auf dem ESXi eingerichtet sein.

Informationen für Windows-Server finden Sie unter [Timekeeping best practices for Windows, including NTP](#).



# Installieren von vRealize Automation mit dem Installationsassistenten

# 3

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 4, „Die vRealize Automation-Standard-Installationsschnittstellen“](#), auf Seite 51.

Dieses Kapitel behandelt die folgenden Themen:

- [„Bereitstellen der vRealize Automation-Appliance“](#), auf Seite 33
- [„Verwenden des Installationsassistenten für minimale Bereitstellungen“](#), auf Seite 35
- [„Verwenden des Installationsassistenten für Unternehmensbereitstellungen“](#), auf Seite 43

## Bereitstellen der vRealize Automation -Appliance

Für die Bereitstellung der vRealize Automation-Appliance muss sich ein Systemadministrator am vSphere-Client anmelden und Bereitstellungseinstellungen auswählen.

Das Root-Kennwort, das Sie für den vRealize Automation-Administrator erstellen, unterliegt gewissen Einschränkungen.

### Voraussetzungen

- Laden Sie die vRealize Automation-Appliance von der VMware-Website herunter.
- Melden Sie sich bei dem vSphere-Client als ein Benutzer mit Systemadministratorrechten an.

### Vorgehensweise

- 1 Wählen Sie **Datei > OVF-Vorlage bereitstellen** aus dem vSphere-Client aus.
- 2 Suchen Sie die heruntergeladene vRealize Automation-Appliance-Datei und klicken Sie auf **Öffnen**.
- 3 Klicken Sie auf **Weiter**.
- 4 Klicken Sie auf der Seite mit den Einzelheiten zur OVF-Vorlage auf **Weiter**.

- 5 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 6 Geben Sie einen eindeutigen Namen für die virtuelle Appliance gemäß der IT-Namenskonvention Ihrer Organisation in das Textfeld **Name** ein, wählen Sie das Datacenter und den Standort aus, für die die virtuelle Appliance bereitgestellt werden soll, und klicken Sie auf **Weiter**.
- 7 Befolgen Sie die Anleitungen, bis die Seite für das Festplattenformat angezeigt wird.
- 8 Überprüfen Sie auf der Seite für das Festplattenformat, dass genügend Speicherplatz zum Bereitstellen der virtuellen Appliance vorhanden ist, und klicken Sie auf **Weiter**.
- 9 Befolgen Sie die Anleitungen, um zur Eigenschaftenseite zu navigieren.  
Die angezeigten Optionen hängen von der vSphere-Konfiguration ab.
- 10 Konfigurieren Sie die Werte auf der Eigenschaftenseite.
  - a Geben Sie das bei der Anmeldung bei der Konsole der virtuellen Appliance zu verwendende Root-Kennwort in die Textfelder **Kennwort eingeben** und **Kennwort bestätigen** ein.
  - b Markieren Sie das Kontrollkästchen **SSH-Dienst** oder heben Sie die Markierung auf, um auszuwählen, ob der SSH-Dienst für die Appliance aktiviert ist.  
  
Dieser Wert wird zum Festlegen des Anfangsstatus des SSH-Diensts in der Appliance verwendet. Wenn Sie den Installationsassistenten für die Installation verwenden, aktivieren Sie diese Option, bevor Sie den Assistenten ausführen. Sie können diese Einstellung nach der Installation über die Appliance-Managementkonsole ändern.
  - c Geben Sie den vollqualifizierten Domännennamen der virtuellen Maschine in das Textfeld **Hostname** ein.
  - d Konfigurieren Sie die Netzwerkeigenschaften.
- 11 Klicken Sie auf **Weiter**.
- 12 Je nach Ihrer Bereitstellungs-, vCenter- und DNS-Konfiguration wählen Sie eines der folgenden Verfahren zum Abschließen der OVA-Bereitstellung und Einschalten der vRealize Automation-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 abgeschlossen ist, klicken Sie auf **Schließen**.
    - c Warten Sie, bis die 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 abgeschlossen ist, klicken Sie auf **Schließen**.
    - b Schalten Sie die vRealize Automation-Appliance ein.
    - c Warten Sie, bis die Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
    - d Stellen Sie sicher, dass Sie das DNS für die vRealize Automation-Appliance anpingen können. Wenn Sie das DNS nicht anpingen können, starten Sie die virtuelle Maschine neu.

- e Warten Sie, bis die 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 Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
- 13 Öffnen Sie eine Eingabeaufforderung und pingen Sie den FQDN an, um zu überprüfen, dass der vollqualifizierte Domänenname für die IP-Adresse von vRealize Automation-Appliance aufgelöst werden kann.

## Verwenden des Installationsassistenten für minimale Bereitstellungen

### Ausführen des Installationsassistenten für eine Minimalbereitstellung

Installieren Sie eine Minimalbereitstellung für Proof-of-Concept-Aufgaben. Der Assistent für eine Minimalinstallation geht davon aus, dass Sie alle IaaS-Komponenten auf einer einzigen Windows-Maschine installieren.

Minimalbereitstellungen unterstützen in der Regel eine einzige vRealize Automation-Appliance, einen IaaS-Server und verwenden einen vSphere-Agent zur Endpoint-Unterstützung.

#### Voraussetzungen

- Vergewissern Sie sich, dass die in [Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“](#), auf Seite 19 beschriebenen Voraussetzungen erfüllt sind.
- [„Bereitstellen der vRealize Automation-Appliance“](#), auf Seite 70

#### Vorgehensweise

- 1 Öffnen Sie einen Webbrowser.
- 2 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 3 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 4 Wenn der Installationsassistent angezeigt wird, klicken Sie auf **Weiter**.
- 5 Akzeptieren Sie die Anwender-Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 6 Wählen Sie im Bildschirm „Bereitstellungstyp“ die Optionen **Minimalbereitstellung** und **Infrastructure-as-a-Service installieren** aus und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie, ob die auf der Seite mit den Installationsvoraussetzungen aufgeführten Voraussetzungen erfüllt sind und ob der Windows Server, auf den Sie den Management-Agent installiert haben, aufgeführt ist.

- 8 Bei Bedarf können Sie die Zeiterfassungsmethode für Ihre vRealize Automation-Appliance ändern. Klicken Sie auf **Zeiteinstellungen ändern**, falls Sie Änderungen vornehmen.
- 9 Klicken Sie auf **Weiter**.
- 10 Klicken Sie im Bildschirm zum Ausführen der Voraussetzungsprüfung auf **Ausführen**, um zu überprüfen, ob der Windows Server in Ihrer Minimalbereitstellung für die Verwendung von vRealize Automation ordnungsgemäß konfiguriert ist.

Dieser Schritt wird im Remotemodus ausgeführt und kann deshalb ein paar Minuten dauern.

- a Falls für eine Maschine ein Fehlerstatus gemeldet wird, klicken Sie auf **Beheben**, um die automatische Korrektur zu starten, oder klicken Sie auf **Details anzeigen** und befolgen Sie die Anweisungen.  
  
Mit der Option **Beheben** werden Korrekturen angewendet, und der IaaS-Windows-Server wird neu gestartet.
  - b Klicken Sie auf **Ausführen**, um die Voraussetzungsprüfung erneut auszuführen.
  - c Klicken Sie auf **Weiter**, wenn alle Status als erfolgreich angezeigt werden.
- 11 Geben Sie in den nachfolgenden Bildschirmen die angeforderten Informationen zum Konfigurieren Ihrer Bereitstellungs-komponenten ein. Hierzu zählen Informationen zum Webserver, Manager Service, Distributed Execution Manager, vSphere-Proxy-Agent und Zertifikat.

Weitere Informationen erhalten Sie über die Hilfeschnittflächen.

#### Weiter

[„Erstellen von Snapshots vor Beginn der Installation“](#), auf Seite 40

## Installieren des Management-Agents

Sie müssen einen Management-Agent auf jeder Windows-Maschine installieren, die IaaS-Komponenten hostet.

Bei Unternehmensinstallationen ist ein Management-Agent für den MS SQL-Host nicht erforderlich.

Wenn Ihre primäre vRealize Automation-Appliance fehlschlägt, müssen Sie Management-Agents neu installieren.

Management-Agents werden nicht automatisch gelöscht, wenn Sie eine IaaS-Komponente deinstallieren. Deinstallieren Sie den Management-Agent wie jedes andere Windows-Programm mit dem Tool „Software“.

#### Vorgehensweise

- 1 [Suchen des Fingerabdrucks für das SSL-Zertifikat des Management-Site-Dienstes](#) auf Seite 36  
Beim Installieren eines Management-Agents müssen Sie den Fingerabdruck des SSL-Zertifikats für den Management-Site-Dienst prüfen.
- 2 [Herunterladen und Installieren eines Management-Agents](#) auf Seite 37  
Ein Administrator lädt den Management-Agent auf die IaaS-Maschine in Ihrer Bereitstellung herunter und installiert ihn. Der Management-Agent muss auf dem IaaS-Server installiert werden. Eine Installation auf dem SQL-Datenbankserver ist nicht erforderlich, wenn dieser getrennt davon vorhanden ist.

### Suchen des Fingerabdrucks für das SSL-Zertifikat des Management-Site-Dienstes

Beim Installieren eines Management-Agents müssen Sie den Fingerabdruck des SSL-Zertifikats für den Management-Site-Dienst prüfen.

Den Fingerabdruck können Sie über die Eingabeaufforderung in der vRealize Automation-Appliance abrufen.

## Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Appliance-Konsole als Root-Benutzer an.
- 2 Geben Sie den folgenden Befehl ein:  
  

```
openssl x509 -in /opt/vmware/etc/httpsd/server.pem -fingerprint -noout -sha1
```

Der SHA1-Fingerabdruck wird angezeigt. Beispiel:  
  

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Kopieren Sie die Fingerabdruck-UID. Zur Validierung müssen Sie möglicherweise die Doppelpunkte entfernen.

## Weiter

Bewahren Sie den kopierten Fingerabdruck für die Verwendung im Management-Agent-Installationsprogramm auf.

## Herunterladen und Installieren eines Management-Agents

Ein Administrator lädt den Management-Agent auf die IaaS-Maschine in Ihrer Bereitstellung herunter und installiert ihn. Der Management-Agent muss auf dem IaaS-Server installiert werden. Eine Installation auf dem SQL-Datenbankserver ist nicht erforderlich, wenn dieser getrennt davon vorhanden ist.

Der Management-Agent registriert den IaaS-Knoten bei der vRealize Automation-Appliance, automatisiert die Installation und Verwaltung von IaaS-Komponenten und erfasst Support- und Telemetriedaten. Der Management-Agent wird auf der IaaS-Maschine als Windows-Dienst ausgeführt, und zum Installieren des Agents benötigen Sie lokale Administratorrechte.

## Voraussetzungen

- Erstellen Sie eine temporäre Kopie des Zertifikat-Fingerabdrucks der vRealize Automation-Appliance, wie in „[Suchen des Fingerabdrucks für das SSL-Zertifikat des Management-Site-Dienstes](#)“, auf Seite 36 beschrieben.
- Vergewissern Sie sich, dass der Benutzer des Dienstkontos ein Domänenkonto mit Administratorrechten auf dem IaaS-Windows-Server ist.

## Vorgehensweise

- 1 Öffnen Sie Ihre vRealize Automation-Appliance, indem Sie eine Adresse in folgendem Format in einem Webbrowser angeben, wobei *vra-va-hostname.domain.name* der vollqualifizierte Domänenname Ihrer vRealize Automation-Appliance ist. Verwenden Sie keine Lastausgleichsdiensadresse.  
  

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 2 Klicken Sie auf das **Installationsprogramm für Management-Agent**, um das Installationsprogramm herunterzuladen.
- 3 Führen Sie das Installationsprogramm für den Management-Agent aus, vCAC-IaaSManagementAgent-Setup.msi.  
  
Der Standardspeicherort ist *%Programme Files(x86)%\VMware\vCAC\Management Agent\*
- 4 Klicken Sie auf der Begrüßungsseite auf **Weiter**.
- 5 Akzeptieren Sie die EULA und klicken Sie auf **Weiter**.
- 6 Geben Sie einen alternativen Installationspfad an oder akzeptieren Sie den Standardwert.
- 7 Klicken Sie auf **Weiter**.

- 8 Geben Sie die Einzelheiten für den Management-Site-Dienst in die folgenden Felder ein und klicken Sie auf **Weiter**.

Textfeld	Input
<b>vRA-Appliance-Adresse</b>	<b>https://vrealize-automation-appliance-FQDN:5480</b> Sie müssen die Portnummer angeben.
<b>Root-Benutzername</b>	Der Root-Benutzer für die vRealize Automation-Appliance.
<b>Kennwort</b>	Das Root-Kennwort für die vRealize Automation-Appliance.
<b>Management-Site-Serverzertifikat</b>	Der SHA1-Fingerabdruck für das Zertifikat des Management-Site-Dienstes. Der Management-Site-Dienst wird auf der vRealize Automation-Appliance gehostet. Beispiel für einen SHA1-Fingerabdruck: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
<b>Laden</b>	Klicken Sie auf <b>Laden</b> , um den Standardfingerabdruck zu laden.

**VMware vRealize Automation Management Agent Setup**

**Management Site Service**

Specify the VA host for the Management Site Service to use for the agent.

vRA appliance address:  
  
 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...

Root username:  Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 9 Aktivieren Sie das Kontrollkästchen **Fingerabdruck-Übereinstimmungsbestätigung**, nachdem Sie bestätigt haben, dass der angezeigte Fingerabdruck mit dem Fingerabdruck des SSL-Zertifikats für die Management-Site übereinstimmt.

Wenn die Fingerabdrücke nicht übereinstimmen, überprüfen Sie, ob die Adresse im Textfeld **vRA-Appliance-Adresse** korrekt ist.

- 10 Klicken Sie auf **Weiter**.
- 11 Geben Sie den Benutzernamen und das Kennwort für das Dienstkonto ein.
- 12 Klicken Sie auf **Weiter**.
- 13 Klicken Sie auf **Installieren**.
- 14 Klicken Sie auf **Fertig stellen**.
- 15 Wiederholen Sie diese Schritte für jeden Windows IaaS-Host.

Nach der Installation des Management-Agents wird der Windows-Server auf der Seite mit den Installationsvoraussetzungen des Installationsassistenten aufgelistet.

## Synchronisieren der Serveruhrzeit

Die Uhren auf vRealize Automation-Servern und Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Mithilfe der Optionen auf der Seite mit den Installationsvoraussetzungen des Installationsassistenten können Sie eine Zeitsynchronisierungsmethode für Ihre virtuellen Appliances auswählen. Die IaaS-Host-Tabelle enthält Informationen zu Zeitversätzen.

### Vorgehensweise

- 1 Wählen Sie eine Option aus dem Menü **Zeitsynchronisierungsmodus** aus.

Option	Aktion
<b>Zeitserver verwenden</b>	Wählen Sie <b>Zeitserver verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um Network Time-Protokoll zu verwenden. Geben Sie für jeden von Ihnen verwendeten Zeitserver die IP-Adresse oder den Hostnamen in das Feld <b>Zeitserver</b> ein.
<b>Hostzeit verwenden</b>	Wählen Sie <b>Hostzeit verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um VMware Tools-Zeitsynchronisierung zu verwenden. Sie müssen die Verbindungen zu NTP-Servern (Network Time Protocol) konfigurieren, bevor Sie die VMware Tools-Zeitsynchronisierung verwenden können.

- 2 Klicken Sie auf **Zeiteinstellungen ändern**.

- 3 Klicken Sie auf **Weiter**.

### Weiter

Vergewissern Sie sich, dass Ihre IaaS-Server ordnungsgemäß konfiguriert sind.

## Ausführen der Voraussetzungsprüfung

Führen Sie die Voraussetzungsprüfung aus, um sicherzustellen, dass der Windows-Server für die IaaS-Komponenten ordnungsgemäß konfiguriert ist.

### Vorgehensweise

- 1 Klicken Sie im Bildschirm zum Ausführen der Voraussetzungsprüfung auf **Ausführen**.

Nachdem die Prüfungen durchgeführt wurden, wird der Windows-Server für IaaS-Komponenten mit einem Status aufgeführt.

- 2 Wenn eine Warnung angezeigt wird, können Sie weitere Informationen zu dem Fehler anfordern oder wählen, dass der Fehler automatisch korrigiert wird.

- ◆ Klicken Sie auf **Details anzeigen**, um weitere Informationen zu dem Fehler anzuzeigen. Außerdem erfahren Sie, mit welchen Maßnahmen Sie den Fehler beheben können.

- ◆ Klicken Sie auf **Beheben**, um den Fehler automatisch beheben zu lassen.

Mit der Option **Beheben** werden Korrekturen angewendet, und der IaaS-Windows-Server wird neu gestartet.

- 3 Klicken Sie auf **Ausführen**, um die Korrekturen zu überprüfen.
- 4 Klicken Sie auf **Weiter**, nachdem alle Fehler behoben wurden.

Ihr Windows-Server ist jetzt ordnungsgemäß für die Installation von IaaS-Komponenten konfiguriert.

## Weiter

Fahren Sie mit dem Host-Bildschirm von vRealize Automation fort.

## Angeben von Parametern für Minimalbereitstellungen

Verwenden Sie den vRealize Automation-Installationsassistenten, um Konfigurationseinstellungen für die Komponenten von Minimalbereitstellungen einzugeben.

### Voraussetzungen

#### Vorgehensweise

- ◆ Befolgen Sie die Seiten des Installationsassistenten, um FQDNs, Kontoanmeldedaten, Kennwörter für Standardmandanten und andere Einstellungen für vRealize Automation-Appliance und IaaS-Windows-Server einzugeben.

Der Assistent überprüft Systeme auf Voraussetzungen, bevor Sie mit der Eingabe von Einstellungen beginnen. Er validiert Ihre Einstellungen, bevor die Produktinstallation gestartet wird.

## Weiter

In vSphere erstellen Sie einen Snapshot von jeder vRealize Automation-Appliance und von IaaS-Windows-Server, bevor die Produktinstallation gestartet wird.

## Erstellen von Snapshots vor Beginn der Installation

Erstellen Sie Snapshots von all Ihren Appliances und Windows-Servern. Wenn die Installation fehlschlägt, können Sie diese Snapshots wiederherstellen und erneut versuchen, die Installation durchzuführen.

Die vorgenommenen Konfigurationseinstellungen werden in den Snapshots beibehalten. Fügen Sie unbedingt auch einen Snapshot der vRealize Automation-Appliance hinzu, auf der der Assistent ausgeführt wird.

Für vSphere-Benutzer gibt es entsprechende Anweisungen.

---

**HINWEIS** Sie sollten den Installationsassistenten nicht beenden bzw. die Installation nicht abbrechen.

---

#### Vorgehensweise

- 1 Öffnen Sie einen anderen Browser und melden Sie sich beim vSphere Client an.
- 2 Suchen Sie in der vSphere Client-Bestandsliste nach Ihrem Server oder Ihrer Appliance.
- 3 Klicken Sie mit der rechten Maustaste auf den Server in der Bestandsliste, und wählen Sie **Snapshot erstellen** aus.
- 4 Geben Sie einen Snapshot-Namen ein.
- 5 Aktivieren Sie das Kontrollkästchen **Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen**, wenn Sie den Arbeitsspeicher des Servers erfassen möchten, und klicken Sie auf **OK**.

Der Snapshot wird erstellt.

Wiederholen Sie diese Schritte, um Snapshots für alle Ihre Server oder Appliances zu erstellen.

## Weiter

[„Abschließen der Installation“](#), auf Seite 64



## Szenario: Abschließen der Installation

Als vSphere-Administrator befinden Sie sich im letzten Teil des Installationsprozesses. Sie beginnen die Installation von vRealize Automation und warten, bis die Installation erfolgreich beendet wurde.

### Vorgehensweise

- 1 Kehren Sie zum Installationsassistenten zurück.
- 2 Überprüfen Sie die Installationsübersicht und klicken Sie auf **Weiter**.
- 3 Geben Sie den Produktlizenzschlüssel ein und klicken Sie auf **Weiter**.
- 4 Akzeptieren oder ändern Sie die Standardtelemetreeinstellungen und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Weiter**.
- 6 Klicken Sie auf **Fertig stellen**.

Die Installation wird gestartet. In Abhängigkeit von Ihrer Netzwerkkonfiguration kann die Installation zwischen fünfzehn Minuten und einer Stunde dauern.

Eine Bestätigungsmeldung wird angezeigt, wenn die Installation abgeschlossen ist.

### Weiter

Jetzt können Sie die Bereitstellung konfigurieren.

## Beheben von Installationsfehlern

Wenn Sie von der Installationsdetailseite aus installieren, werden Sie über alle Probleme informiert, die einen Abschluss der Installation verhindern.

Wenn Probleme gefunden werden, wird die Komponente markiert, und Sie erhalten ausführliche Informationen zum Fehler sowie zu Schritten für eine Prüfung und Behebung. Nachdem Sie das Problem behoben haben, versuchen Sie den Installationsschritt erneut. Je nach Problemtyp führen Sie verschiedene Behebungsschritte aus.

### Vorgehensweise

- 1 Wenn die Schaltfläche **Fehlgeschlagene wiederholen** aktiviert ist, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, welche Änderungen erforderlich sind, und führen Sie sie durch.
  - c Kehren Sie zum Installationsbildschirm zurück und klicken Sie auf **Fehlgeschlagene wiederholen**.  
Das Installationsprogramm versucht, alle fehlgeschlagenen Komponenten zu installieren.
- 2 Wenn die Schaltfläche **Alle IaaS wiederholen** aktiviert ist, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, was geändert werden muss.
  - c Stellen Sie für alle IaaS-Server die zuvor erstellten Snapshots wieder her.
  - d Löschen Sie die MS SQL-Datenbank, falls Sie eine externe Datenbank verwenden.
  - e Nehmen Sie die erforderlichen Änderungen vor.
  - f Klicken Sie auf **Alle IaaS wiederholen**.

- 3 Wenn der Fehler an den Komponenten der virtuellen Appliance liegt, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, was geändert werden muss.
  - c Stellen Sie alle Server auf die Snapshots wieder her, einschließlich desjenigen, auf dem Sie den Assistenten ausführen.
  - d Nehmen Sie die erforderlichen Änderungen vor.
  - e Aktualisieren Sie die Seite des Assistenten.
  - f Melden Sie sich an und führen Sie den Assistenten erneut aus.

Der Assistent wird mit dem Schritt vor der Installation geöffnet.

## Einrichten der Anmeldedaten für die Erstkonfiguration von Inhalten

Sie können auch einen Workflow für den anfänglichen Inhalt für einen vSphere-Endpoint starten.

Bei diesem Prozess wird der lokale Benutzer „configurationadmin“ verwendet, dem Administratorrechte erteilt werden.

### Vorgehensweise

- 1 Im Textfeld **Kennwort** müssen Sie ein Kennwort für das Konto „configurationadmin“ erstellen und eingeben.
- 2 Geben Sie das Kennwort im Textfeld **Kennwort bestätigen** erneut ein. Notieren Sie sich das Kennwort für die spätere Verwendung.
- 3 Klicken Sie auf **Ausgangsinhalt erstellen**.
- 4 Klicken Sie auf **Weiter**.

Ein Konfigurationsadministrator-Benutzer wird erstellt und ein Konfigurationskatalogelement wird im Standardmandanten erstellt. Dem Konfigurationsadministrator werden die folgenden Rechte erteilt:

- Genehmigungsadministrator
- Katalog-Administrator
- IaaS-Administrator
- Infrastrukturarchitekt
- Mandantenadministrator
- XaaS-Architekt

### Weiter

- Wenn Sie den Assistenten beenden, können Sie sich beim Standardmandanten als configurationadmin-Benutzer anmelden und die Katalogelemente für den anfänglichen Inhalt anfordern. Ein Beispiel für das Anfordern des Elements und das Abschließen der manuellen Benutzeraktion finden Sie unter *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.
- Konfigurieren Sie den Zugriff auf den Standardmandanten für andere Benutzer. Siehe [„Konfigurieren des Zugriffs auf den Standardmandanten“](#), auf Seite 129.

## 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-Appliance-Appliances ein Fehlschlagen der Installation. Nur eine einzige Webserverinstanz und eine vRealize Automation-Appliance dürfen während der Installation aktiv sein.

## Ausführen des Installationsassistenten für eine Unternehmensbereitstellung

Unternehmensbereitstellungen werden für die Produktionsumgebung verwendet. Mit dem Installationsassistenten können Sie eine verteilte Installation oder eine verteilte Installation mit Lastausgleichsdiensten zur Unterstützung von High Availability und Failover bereitstellen.

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.

### Voraussetzungen

- Vergewissern Sie sich, dass die in [Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“](#), auf Seite 19 beschriebenen Voraussetzungen erfüllt sind.
- [„Bereitstellen der vRealize Automation-Appliance“](#), auf Seite 70.

### Vorgehensweise

- 1 Öffnen Sie vRealize Automation-Appliance in einem Webbrowser. Verwenden Sie den vollqualifizierten Domännennamen (FQDN).  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Melden Sie sich als Root-Benutzer an und verwenden Sie das bei der OVA-Bereitstellung erstellte Kennwort.  
  
Bei der ersten Anmeldung wird der Installationsassistent angezeigt.
- 3 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
- 4 Wählen Sie auf der Seite „Bereitstellungstyp“ **Unternehmensbereitstellung** und **Infrastructure as a Service installieren** aus.
- 5 Auf der Seite „Installationsvoraussetzungen“ melden Sie sich bei den IaaS Windows-Servern an und installieren den Management-Agent. Der Management-Agent lässt zu, dass der Assistent diese IaaS-Server erkennt und eine Verbindung zu ihnen herstellt.

### Weiter

Siehe [„Installieren des Management-Agents“](#), auf Seite 44.

## Installieren des Management-Agents

Sie müssen einen Management-Agent auf jeder Windows-Maschine installieren, die IaaS-Komponenten hostet.

Wenn Ihre primäre vRealize Automation-Appliance fehlschlägt, müssen Sie Management-Agents neu installieren.

Management-Agents werden nicht automatisch gelöscht, wenn Sie eine IaaS-Komponente deinstallieren. Deinstallieren Sie den Management-Agent wie jedes andere Windows-Programm mit dem Tool „Software“.

### Suchen des Fingerabdrucks für das SSL-Zertifikat des Management-Site-Dienstes

Beim Installieren eines Management-Agents müssen Sie den Fingerabdruck des SSL-Zertifikats für den Management-Site-Dienst prüfen.

Den Fingerabdruck können Sie über die Eingabeaufforderung in der vRealize Automation-Appliance abrufen.

#### Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Appliance-Konsole als Root-Benutzer an.
- 2 Geben Sie den folgenden Befehl ein:  

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

 Der SHA1-Fingerabdruck wird angezeigt. Beispiel:  

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Kopieren Sie die Fingerabdruck-UID. Zur Validierung müssen Sie möglicherweise die Doppelpunkte entfernen.

#### Weiter

Bewahren Sie den kopierten Fingerabdruck für die Verwendung im Management-Agent-Installationsprogramm auf.

### Herunterladen und Installieren eines Management-Agents

Ein Administrator lädt einen Management-Agent auf IaaS-Maschinen in Ihrer Bereitstellung herunter und installiert sie. Der Management-Agent muss auf allen IaaS-Servern installiert werden, mit Ausnahme derjenigen, die ausschließlich für Ihre MS SQL-Datenbank verwendet werden.

Der Management-Agent registriert IaaS-Knoten bei der vRealize Automation-Appliance, automatisiert die Installation und Verwaltung von IaaS-Komponenten und erfasst Support- und Telemetriedaten. Der Management-Agent wird auf der IaaS-Maschine als Windows-Dienst ausgeführt, und zum Installieren des Agents benötigen Sie lokale Administratorrechte.

#### Voraussetzungen

- Erstellen Sie eine temporäre Kopie des Zertifikat-Fingerabdrucks der vRealize Automation-Appliance, wie in [„Suchen des Fingerabdrucks für das SSL-Zertifikat des Management-Site-Dienstes“](#), auf Seite 36 beschrieben.
- Vergewissern Sie sich, dass der Benutzer des Dienstkontos ein Domänenkonto mit Administratorrechten auf dem IaaS-Windows-Server ist.

## Vorgehensweise

- 1 Öffnen Sie Ihre vRealize Automation-Appliance, indem Sie eine Adresse in folgendem Format in einem Webbrowser angeben, wobei *vra-va-hostname.domain.name* der vollqualifizierte Domänenname Ihrer vRealize Automation-Appliance ist. Verwenden Sie keine Lastausgleichsdiensadresse.

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

- 2 Klicken Sie auf das **Installationsprogramm für Management-Agent**, um das Installationsprogramm herunterzuladen.
- 3 Führen Sie das Installationsprogramm für den Management-Agent aus, vCAC-IaaSManagementAgent-Setup.msi.  
Der Standardspeicherort ist `%Programme Files(x86)%\VMware\vCAC\Management Agent\`
- 4 Klicken Sie auf der Begrüßungsseite auf **Weiter**.
- 5 Akzeptieren Sie die EULA und klicken Sie auf **Weiter**.
- 6 Geben Sie einen alternativen Installationspfad an oder akzeptieren Sie den Standardwert.
- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie die Einzelheiten für den Management-Site-Dienst in die folgenden Felder ein und klicken Sie auf **Weiter**.

Textfeld	Input
<b>vRA-Appliance-Adresse</b>	<code>https://vrealize-automation-appliance-FQDN:5480</code> Sie müssen die Portnummer angeben.
<b>Root-Benutzername</b>	Der Root-Benutzer für die vRealize Automation-Appliance.
<b>Kennwort</b>	Das Root-Kennwort für die vRealize Automation-Appliance.

Textfeld	Input
<b>Management-Site-Serverzertifikat</b>	Der SHA1-Fingerabdruck für das Zertifikat des Management-Site-Dienstes. Der Management-Site-Dienst wird auf der vRealize Automation-Appliance gehostet. Beispiel für einen SHA1-Fingerabdruck: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
<b>Laden</b>	Klicken Sie auf <b>Laden</b> , um den Standardfingerabdruck zu laden.

The screenshot shows the 'Management Site Service' configuration window. It includes fields for 'vRA appliance address' (with a hint to specify scheme and port), 'Root username' (set to 'root'), and 'Password'. Below these is a 'Management Site Service certificate SHA1 fingerprint' field containing the value '4F03BF5B12D49E351B2F6C779B2B1C2A4D10E882' and a 'Load' button. A checkbox is checked with the text 'I confirm the fingerprint matches the Management Site Service SSL certificate'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- 9 Aktivieren Sie das Kontrollkästchen **Fingerabdruck-Übereinstimmungsbestätigung**, nachdem Sie bestätigt haben, dass der angezeigte Fingerabdruck mit dem Fingerabdruck des SSL-Zertifikats für die Management-Site übereinstimmt.

Wenn die Fingerabdrücke nicht übereinstimmen, überprüfen Sie, ob die Adresse im Textfeld **vRA-Appliance-Adresse** korrekt ist.

- 10 Klicken Sie auf **Weiter**.
- 11 Geben Sie den Benutzernamen und das Kennwort für das Dienstkonto ein.
- 12 Klicken Sie auf **Weiter**.
- 13 Klicken Sie auf **Installieren**.
- 14 Klicken Sie auf **Fertig stellen**.
- 15 Wiederholen Sie diese Schritte für jeden Windows IaaS-Host.

Nach der Installation des Management-Agents wird der Windows-Server auf der Seite mit den Installationsvoraussetzungen des Installationsassistenten aufgelistet.

## Synchronisieren der Serveruhrzeit

Die Uhren auf vRealize Automation-Servern und Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Mithilfe der Optionen auf der Seite mit den Installationsvoraussetzungen des Installationsassistenten können Sie eine Zeitsynchronisierungsmethode für Ihre virtuellen Appliances auswählen. Die IaaS-Host-Tabelle enthält Informationen zu Zeitversätzen.

### Vorgehensweise

- 1 Wählen Sie eine Option aus dem Menü **Zeitsynchronisierungsmodus** aus.

Option	Aktion
<b>Zeitserver verwenden</b>	Wählen Sie <b>Zeitserver verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um Network Time-Protokoll zu verwenden. Geben Sie für jeden von Ihnen verwendeten Zeitserver die IP-Adresse oder den Hostnamen in das Feld <b>Zeitserver</b> ein.
<b>Hostzeit verwenden</b>	Wählen Sie <b>Hostzeit verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um VMware Tools-Zeitsynchronisierung zu verwenden. Sie müssen die Verbindungen zu NTP-Servern (Network Time Protocol) konfigurieren, bevor Sie die VMware Tools-Zeitsynchronisierung verwenden können.

- 2 Klicken Sie auf **Zeiteinstellungen ändern**.
- 3 Klicken Sie auf **Weiter**.

### Weiter

Vergewissern Sie sich, dass Ihre IaaS-Server ordnungsgemäß konfiguriert sind.

## Ausführen der Voraussetzungsprüfung

Führen Sie die Voraussetzungsprüfung aus, um sicherzustellen, dass die IaaS-Komponenten für die Windows-Server ordnungsgemäß konfiguriert sind.

### Vorgehensweise

- 1 Klicken Sie im Bildschirm zum Ausführen der Voraussetzungsprüfung auf **Ausführen**.  
Nachdem die Prüfungen durchgeführt wurden, ist jede IaaS-Komponente für die Windows-Server mit einem Status aufgeführt.
- 2 Wenn eine Warnung angezeigt wird, können Sie weitere Informationen zu dem Fehler anfordern oder wählen, dass der Fehler automatisch korrigiert wird.
  - ◆ Klicken Sie auf **Details anzeigen**, um weitere Informationen zu dem Fehler anzuzeigen. Außerdem erfahren Sie, mit welchen Maßnahmen Sie den Fehler beheben können.
  - ◆ Klicken Sie auf **Beheben**, um den Fehler automatisch beheben zu lassen.  
Mit der Option **Beheben** werden Korrekturen angewendet und alle IaaS-Maschinen werden neu gestartet, einschließlich der Maschinen, für die keine Korrekturen vorgenommen wurden.
- 3 Klicken Sie auf **Ausführen**, um die Korrekturen zu überprüfen.
- 4 Klicken Sie auf **Weiter**, nachdem alle Fehler behoben wurden.

Ihre Windows-Server sind jetzt ordnungsgemäß für die Installation von IaaS-Komponenten konfiguriert.

## Weiter

Fahren Sie mit dem Host-Bildschirm von vRealize Automation fort.

## Angeben von Parametern für Unternehmensbereitstellungen

Verwenden Sie den vRealize Automation-Installationsassistenten, um Konfigurationseinstellungen für die Komponenten von Unternehmensbereitstellungen einzugeben.

### Voraussetzungen

#### Vorgehensweise

- ◆ Befolgen Sie die Seiten des Installationsassistenten, um FQDNs, Kontoanmeldedaten, Kennwörter für Standardmandanten und andere Einstellungen für vRealize Automation-Appliance und IaaS-Windows-Server einzugeben.

Der Assistent überprüft Systeme auf Voraussetzungen, bevor Sie mit der Eingabe von Einstellungen beginnen. Er validiert Ihre Einstellungen, bevor die Produktinstallation gestartet wird.

## Weiter

In vSphere erstellen Sie einen Snapshot von jeder vRealize Automation-Appliance und von IaaS-Windows-Server, bevor die Produktinstallation gestartet wird.

## Erstellen von Snapshots vor Beginn der Installation

Erstellen Sie Snapshots von all Ihren Appliances und Windows-Servern. Wenn die Installation fehlschlägt, können Sie diese Snapshots wiederherstellen und erneut versuchen, die Installation durchzuführen.

Die vorgenommenen Konfigurationseinstellungen werden in den Snapshots beibehalten. Fügen Sie unbedingt auch einen Snapshot der vRealize Automation-Appliance hinzu, auf der der Assistent ausgeführt wird.

Für vSphere-Benutzer gibt es entsprechende Anweisungen.

---

**HINWEIS** Sie sollten den Installationsassistenten nicht beenden bzw. die Installation nicht abbrechen.

---

#### Vorgehensweise

- 1 Öffnen Sie einen anderen Browser und melden Sie sich beim vSphere Client an.
- 2 Suchen Sie in der vSphere Client-Bestandsliste nach Ihrem Server oder Ihrer Appliance.
- 3 Klicken Sie mit der rechten Maustaste auf den Server in der Bestandsliste, und wählen Sie **Snapshot erstellen** aus.
- 4 Geben Sie einen Snapshot-Namen ein.
- 5 Aktivieren Sie das Kontrollkästchen **Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen**, wenn Sie den Arbeitsspeicher des Servers erfassen möchten, und klicken Sie auf **OK**.

Der Snapshot wird erstellt.

Wiederholen Sie diese Schritte, um Snapshots für alle Ihre Server oder Appliances zu erstellen.

## Weiter

[„Abschließen der Installation“](#), auf Seite 64



## Abschließen der Installation

Nach dem Erstellen der Snapshots können Sie mit der Installation von vRealize Automation beginnen und warten, bis die Installation erfolgreich abgeschlossen wurde.

### Vorgehensweise

- 1 Kehren Sie zum Installationsassistenten zurück.
- 2 Überprüfen Sie die Installationsübersicht und klicken Sie auf **Weiter**.
- 3 Klicken Sie auf **Weiter**.
- 4 Klicken Sie auf **Fertig stellen**.

Die Installation wird gestartet. In Abhängigkeit von Ihrer Netzwerkkonfiguration kann die Installation zwischen fünfzehn Minuten und einer Stunde dauern.

Eine Bestätigungsmeldung wird angezeigt, wenn die Installation abgeschlossen ist.

### Weiter

Jetzt können Sie die Bereitstellung konfigurieren.

## Beheben von Installationsfehlern

Wenn Sie von der Installationsdetailseite aus installieren, werden Sie über alle Probleme informiert, die einen Abschluss der Installation verhindern.

Wenn Probleme gefunden werden, wird die Komponente markiert, und Sie erhalten ausführliche Informationen zum Fehler sowie zu Schritten für eine Prüfung und Behebung. Nachdem Sie das Problem behoben haben, versuchen Sie den Installationsschritt erneut. Je nach Problemtyp führen Sie verschiedene Behebungsschritte aus.

### Vorgehensweise

- 1 Wenn die Schaltfläche **Fehlgeschlagene wiederholen** aktiviert ist, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, welche Änderungen erforderlich sind, und führen Sie sie durch.
  - c Kehren Sie zum Installationsbildschirm zurück und klicken Sie auf **Fehlgeschlagene wiederholen**.  
Das Installationsprogramm versucht, alle fehlgeschlagenen Komponenten zu installieren.
- 2 Wenn die Schaltfläche **Alle IaaS wiederholen** aktiviert ist, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, was geändert werden muss.
  - c Stellen Sie für alle IaaS-Server die zuvor erstellten Snapshots wieder her.
  - d Löschen Sie die MS SQL-Datenbank, falls Sie eine externe Datenbank verwenden.
  - e Nehmen Sie die erforderlichen Änderungen vor.
  - f Klicken Sie auf **Alle IaaS wiederholen**.

- 3 Wenn der Fehler an den Komponenten der virtuellen Appliance liegt, verwenden Sie die folgenden Schritte.
  - a Prüfen Sie den Fehler.
  - b Bewerten Sie, was geändert werden muss.
  - c Stellen Sie alle Server auf die Snapshots wieder her, einschließlich desjenigen, auf dem Sie den Assistenten ausführen.
  - d Nehmen Sie die erforderlichen Änderungen vor.
  - e Aktualisieren Sie die Seite des Assistenten.
  - f Melden Sie sich an und führen Sie den Assistenten erneut aus.

Der Assistent wird mit dem Schritt vor der Installation geöffnet.

## Einrichten der Anmeldedaten für die Erstkonfiguration von Inhalten

Sie können auch einen Workflow für den anfänglichen Inhalt für einen vSphere-Endpoint starten.

Bei diesem Prozess wird der lokale Benutzer „configurationadmin“ verwendet, dem Administratorrechte erteilt werden.

### Vorgehensweise

- 1 Im Textfeld **Kennwort** müssen Sie ein Kennwort für das Konto „configurationadmin“ erstellen und eingeben.
- 2 Geben Sie das Kennwort im Textfeld **Kennwort bestätigen** erneut ein. Notieren Sie sich das Kennwort für die spätere Verwendung.
- 3 Klicken Sie auf **Ausgangsinhalt erstellen**.
- 4 Klicken Sie auf **Weiter**.

Ein Konfigurationsadministrator-Benutzer wird erstellt und ein Konfigurationskatalogelement wird im Standardmandanten erstellt. Dem Konfigurationsadministrator werden die folgenden Rechte erteilt:

- Genehmigungsadministrator
- Katalog-Administrator
- IaaS-Administrator
- Infrastrukturarchitekt
- Mandantenadministrator
- XaaS-Architekt

### Weiter

- Wenn Sie den Assistenten beenden, können Sie sich beim Standardmandanten als configurationadmin-Benutzer anmelden und die Katalogelemente für den anfänglichen Inhalt anfordern. Ein Beispiel für das Anfordern des Elements und das Abschließen der manuellen Benutzeraktion finden Sie unter *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.
- Konfigurieren Sie den Zugriff auf den Standardmandanten für andere Benutzer. Siehe [„Konfigurieren des Zugriffs auf den Standardmandanten“](#), auf Seite 129.

# Die vRealize Automation -Standard-Installationsschnittstellen

---

# 4

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

Der unter [Kapitel 3, „Installieren von vRealize Automation mit dem Installationsassistenten“](#), auf Seite 33 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 aus irgendeinem Grund 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 behandelt die folgenden Themen:

- [„Verwenden der Standardschnittstellen für minimale Bereitstellungen“](#), auf Seite 51
- [„Verwenden der Standardschnittstellen für verteilte Bereitstellungen“](#), auf Seite 64
- [„Installieren der vRealize Automation-Agents“](#), auf Seite 104

## 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

Ein Systemadministrator kann eine vollständige vRealize Automation-Instanz in einer Minimalkonfiguration bereitstellen. Minimalbereitstellungen werden normalerweise in einer Entwicklungsumgebung oder als Machbarkeitsnachweis verwendet. Für die Installation sind weniger Schritte erforderlich.

Die Checkliste für die Minimalbereitstellung bietet einen allgemeinen Überblick über die Abfolge der Aufgaben, die Sie zum Abschließen einer Minimalinstallation durchführen müssen.

Drucken Sie eine Kopie der Checkliste aus und verwenden Sie sie als Leitfaden für die Durchführung der Installation. Führen Sie die Aufgaben in der Reihenfolge aus, in der sie vorgegeben werden.

**Tabelle 4-1.** Checkliste für Minimalbereitstellung

Aufgabe	Details
<input type="checkbox"/> Planen Sie die Installationsumgebung und bereiten Sie sie vor. Stellen Sie sicher, dass alle Installationsvoraussetzungen erfüllt sind.	<a href="#">Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“</a> , auf Seite 19
<input type="checkbox"/> Richten Sie Ihre vRealize Automation-Appliance ein.	<a href="#">„Bereitstellen und Konfigurieren der vRealize Automation-Appliance“</a> , auf Seite 52
<input type="checkbox"/> Installieren Sie IaaS-Komponenten auf einem einzelnen Windows Server.	<a href="#">„Installieren der IaaS-Komponenten“</a> , auf Seite 58
<input type="checkbox"/> Installieren Sie zusätzliche Agents, falls erforderlich.	<a href="#">„Installieren der vRealize Automation-Agents“</a> , auf Seite 104
<input type="checkbox"/> Führen Sie Aufgaben nach der Installation aus, wie beispielsweise das Konfigurieren des Standardmandanten.	

## Bereitstellen und Konfigurieren der vRealize Automation -Appliance

Die vRealize Automation-Appliance ist eine vorkonfigurierte virtuelle Appliance, die den vRealize Automation-Appliance-Server und die Webkonsole (das Benutzerportal) bereitstellt. Sie wird als Open Virtualization Format (OVF)-Vorlage bereitgestellt. Der Systemadministrator lädt die Appliance herunter und stellt sie in der vCenter Server- oder ESX/ESXi-Bestandsliste bereit.

### 1 [Bereitstellen der vRealize Automation-Appliance](#) auf Seite 52

Für die Bereitstellung der vRealize Automation-Appliance muss sich ein Systemadministrator am vSphere-Client anmelden und Bereitstellungseinstellungen auswählen.

### 2 [Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance](#) auf Seite 54

Die Uhren auf dem vRealize Automation-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

### 3 [Konfigurieren der vRealize Automation-Appliance](#) auf Seite 55

Zur Vorbereitung der vRealize Automation-Appliance für die Verwendung konfiguriert ein Systemadministrator die Hosteinstellungen, generiert ein SSL-Zertifikat und stellt SSO-Verbindungsinformationen bereit.

## Bereitstellen der vRealize Automation -Appliance

Für die Bereitstellung der vRealize Automation-Appliance muss sich ein Systemadministrator am vSphere-Client anmelden und Bereitstellungseinstellungen auswählen.

Das Root-Kennwort, das Sie für den vRealize Automation-Administrator erstellen, unterliegt gewissen Einschränkungen.

## Voraussetzungen

- Laden Sie die vRealize Automation-Appliance von der VMware-Website herunter.
- Melden Sie sich bei dem vSphere-Client als ein Benutzer mit Systemadministratorrechten an.

## Vorgehensweise

- 1 Wählen Sie **Datei > OVF-Vorlage bereitstellen** aus dem vSphere-Client aus.
- 2 Suchen Sie die heruntergeladene vRealize Automation-Appliance-Datei und klicken Sie auf **Öffnen**.
- 3 Klicken Sie auf **Weiter**.
- 4 Klicken Sie auf der Seite mit den Einzelheiten zur OVF-Vorlage auf **Weiter**.
- 5 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 6 Geben Sie einen eindeutigen Namen für die virtuelle Appliance gemäß der IT-Namenskonvention Ihrer Organisation in das Textfeld **Name** ein, wählen Sie das Datencenter und den Standort aus, für die die virtuelle Appliance bereitgestellt werden soll, und klicken Sie auf **Weiter**.
- 7 Befolgen Sie die Anleitungen, bis die Seite für das Festplattenformat angezeigt wird.
- 8 Überprüfen Sie auf der Seite für das Festplattenformat, dass genügend Speicherplatz zum Bereitstellen der virtuellen Appliance vorhanden ist, und klicken Sie auf **Weiter**.
- 9 Befolgen Sie die Anleitungen, um zur Eigenschaftenseite zu navigieren.  
Die angezeigten Optionen hängen von der vSphere-Konfiguration ab.
- 10 Konfigurieren Sie die Werte auf der Eigenschaftenseite.
  - a Geben Sie das bei der Anmeldung bei der Konsole der virtuellen Appliance zu verwendende Root-Kennwort in die Textfelder **Kennwort eingeben** und **Kennwort bestätigen** ein.
  - b Markieren Sie das Kontrollkästchen **SSH-Dienst** oder heben Sie die Markierung auf, um auszuwählen, ob der SSH-Dienst für die Appliance aktiviert ist.  
  
Dieser Wert wird zum Festlegen des Anfangsstatus des SSH-Diensts in der Appliance verwendet. Wenn Sie den Installationsassistenten für die Installation verwenden, aktivieren Sie diese Option, bevor Sie den Assistenten ausführen. Sie können diese Einstellung nach der Installation über die Appliance-Managementkonsole ändern.
  - c Geben Sie den vollqualifizierten Domännennamen der virtuellen Maschine in das Textfeld **Hostname** ein.
  - d Konfigurieren Sie die Netzwerkeigenschaften.
- 11 Klicken Sie auf **Weiter**.
- 12 Je nach Ihrer Bereitstellungs-, vCenter- und DNS-Konfiguration wählen Sie eines der folgenden Verfahren zum Abschließen der OVA-Bereitstellung und Einschalten der vRealize Automation-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 abgeschlossen ist, klicken Sie auf **Schließen**.

- c Warten Sie, bis die 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 abgeschlossen ist, klicken Sie auf **Schließen**.
    - b Schalten Sie die vRealize Automation-Appliance ein.
    - c Warten Sie, bis die Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
    - d Stellen Sie sicher, dass Sie das DNS für die vRealize Automation-Appliance anpingen können. Wenn Sie das DNS nicht anpingen können, starten Sie die virtuelle Maschine neu.
    - e Warten Sie, bis die 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 Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
- 13 Öffnen Sie eine Eingabeaufforderung und pingen Sie den FQDN an, um zu überprüfen, dass der vollqualifizierte Domänenname für die IP-Adresse von vRealize Automation-Appliance aufgelöst werden kann.

## Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance

Die Uhren auf dem vRealize Automation-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

### Voraussetzungen

„Bereitstellen der vRealize Automation-Appliance“, auf Seite 33.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 3 Wählen Sie **Administrator > Uhrzeiteinstellungen** aus.

- 4 Wählen Sie eine Option aus dem Menü **Zeitsynchronisierungsmodus** aus.

Option	Aktion
<b>Zeitserver verwenden</b>	Wählen Sie <b>Zeitserver verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um Network Time-Protokoll zu verwenden. Geben Sie für jeden von Ihnen verwendeten Zeitserver die IP-Adresse oder den Hostnamen in das Feld <b>Zeitserver</b> ein.
<b>Hostzeit verwenden</b>	Wählen Sie <b>Hostzeit verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um VMware Tools-Zeitsynchronisierung zu verwenden. Sie müssen die Verbindungen zu NTP-Servern (Network Time Protocol) konfigurieren, bevor Sie die VMware Tools-Zeitsynchronisierung verwenden können.

- 5 Klicken Sie auf **Einstellungen speichern**.
- 6 Klicken Sie auf **Aktualisieren**.
- 7 Überprüfen Sie, dass der Wert in **Aktuelle Uhrzeit** richtig ist.
- Sie können die Zeitzone bei Bedarf auf der Seite für die Zeitzoneneinstellung auf der Registerkarte **System** ändern.
- 8 (Optional) Klicken Sie auf **Zeitzone** auf der Registerkarte **System** und wählen Sie eine Zeitzone für das System aus den Menüoptionen aus.
- Der Standardwert ist Etc/UTC.
- 9 Klicken Sie auf **Einstellungen speichern**.

## Konfigurieren der vRealize Automation -Appliance

Zur Vorbereitung der vRealize Automation-Appliance für die Verwendung konfiguriert ein Systemadministrator die Hosteinstellungen, generiert ein SSL-Zertifikat und stellt SSO-Verbindungsinformationen bereit.

### Voraussetzungen

„Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance“, auf Seite 54.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Setzen Sie den Vorgang unabhängig von der Zertifikatswarnung fort.
- 3 Melden Sie sich mit dem Benutzernamen „root“ und dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

- 4 Wählen Sie **vRA-Einstellungen > Hosteinstellungen** aus.

Option	Aktion
<b>Automatisch lösen</b>	Wählen Sie <b>Automatisch lösen</b> aus, um den Namen des aktuellen Hosts für die vRealize Automation-Appliance anzugeben.
<b>Host aktualisieren</b>	<p>Wählen Sie für neue Hosts die Option <b>Host aktualisieren</b> aus. Geben Sie den vollqualifizierten Domännennamen der vRealize Automation-Appliance, <i>vra-hostname.domain.name</i>, in das Textfeld <b>Hostname</b> ein.</p> <p>Wählen Sie für verteilte Bereitstellungen mit Lastausgleichsdiensten die Option <b>Host aktualisieren</b> aus. Geben Sie den vollqualifizierten Domännennamen für den Lastausgleichsserver, <i>vra-loadbalancername.domain.name</i>, in das Textfeld <b>Hostname</b> ein.</p>

**HINWEIS** Konfigurieren Sie SSO-Einstellungen gemäß der Beschreibung weiter unten in diesem Verfahren immer dann, wenn Sie **Host aktualisieren** zum Festlegen des Hostnamens verwenden.



- 5 Wählen Sie aus dem Menü **Zertifikatsaktion** den Zertifikatstyp aus.

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

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

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

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

Option	Aktion
<b>Vorhandene beibehalten</b>	Behalten Sie die aktuelle SSL-Konfiguration bei. Wählen Sie diese Option zum Verwerfen der Änderungen.
<b>Zertifikat generieren</b>	<ul style="list-style-type: none"> <li>a Der im Textfeld <b>Allgemeiner Name</b> 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.</li> <li>b Geben Sie den Namen Ihrer Organisation, wie z. B. den Unternehmensnamen, in das Textfeld <b>Organisation</b> ein.</li> <li>c Geben Sie Ihre Organisationseinheit, wie z. B. den Namen oder den Standort Ihrer Abteilung, in das Textfeld <b>Organisationseinheit</b> ein.</li> <li>d Geben Sie eine zweistellige Landeskennzahl nach ISO 3166 wie z. B. <b>DE</b> in das Textfeld <b>Land</b> ein.</li> </ul>
<b>Importieren</b>	<ul style="list-style-type: none"> <li>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 <b>RSA-Privatschlüssel</b> ein.</li> <li>b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld <b>Zertifikatskette</b> ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu.  <b>HINWEIS</b> Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</li> <li>c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld <b>Passphrase</b> ein.</li> </ul>

- 6 Klicken Sie auf **Einstellungen speichern**, um Hostinformationen und SSL-Konfiguration zu speichern.
- 7 Konfigurieren Sie die SSO-Einstellungen.
- 8 Klicken Sie auf **Messaging**. Die Konfigurationseinstellungen und der Status des Messaging für Ihre Appliance werden angezeigt. Ändern Sie diese Einstellungen nicht.

- 9 Klicken Sie auf die Registerkarte **Telemetrie**, um auszuwählen, ob Sie am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program, CEIP) von VMware teilnehmen möchten.

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

- Aktivieren Sie **Join the VMware Customer Experience Improvement Program**, um an diesem Programm teilzunehmen.
- Deaktivieren Sie **Join the VMware Customer Experience Improvement Program**, um nicht an diesem Programm teilzunehmen.

- 10 Klicken Sie auf **Services** und stellen Sie sicher, dass Dienste registriert sind.

Je nach Site-Konfiguration kann dies etwa 10 Minuten dauern.

---

**HINWEIS** Sie können sich bei der Appliance anmelden und `tail -f /var/log/vcac/catalina.out` ausführen, um das Starten der Dienste zu überwachen.

---

- 11 Geben Sie Ihre Lizenzinformationen ein.

- a Klicken Sie auf **vRA-Einstellungen > Lizenzierung**.
- b Klicken Sie auf **Lizenzierung**.
- c Geben Sie einen gültigen vRealize Automation-Lizenzschlüssel ein, den Sie beim Herunterladen der Installationsdateien heruntergeladen haben, und klicken Sie auf **Schlüssel senden**.

---

**HINWEIS** Wenn ein Verbindungsfehler auftritt, liegt möglicherweise ein Problem mit dem Lastausgleichsdienst vor. Überprüfen Sie die Netzwerkkonnektivität zum Lastausgleichsdienst.

---

- 12 Überprüfen Sie, ob Sie sich an der vRealize Automation-Konsole anmelden können.

- a Öffnen Sie einen Browser und navigieren Sie zu `https://vcac-hostname.domain.name/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 Konsole wird auf der Seite „Mandanten“ auf der Registerkarte **Administration** geöffnet. Ein einzelner Mandant mit dem Namen `vsphere.local` wird in der Liste angezeigt.

Sie haben die Bereitstellung und Konfiguration Ihrer vRealize Automation-Appliance abgeschlossen. Wenn die Appliance nach der Konfiguration nicht ordnungsgemäß funktioniert, stellen Sie die Appliance erneut bereit und konfigurieren Sie sie neu. Nehmen Sie bei der vorhandenen Appliance keine Änderungen vor.

#### Weiter

[„Installieren der Infrastrukturkomponenten“](#), auf Seite 59

## 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.

### Vorgehensweise

- 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“](#), auf Seite 81 im Kapitel zu verteilten Bereitstellungen.

## Installieren der Infrastrukturkomponenten

Der Systemadministrator meldet sich bei der Windows-Maschine an und folgt dem Installationsassistenten zum Installieren der Infrastrukturkomponenten (IaaS) auf der virtuellen oder physischen Windows-Maschine.

### Voraussetzungen

- Stellen Sie sicher, dass die Installationsmaschine die Anforderungen erfüllt, die in [„Anforderungen an den IaaS-Webdienst und den Model Manager-Server“](#), auf Seite 22 beschrieben sind.
- [„Aktivieren der Zeitsynchronisierung auf dem Windows-Server“](#), auf Seite 59.
- 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).

### Vorgehensweise

- 1 [Herunterladen des Installationsprogramms für vRealize Automation IaaS](#) auf Seite 60  
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](#) auf Seite 60  
Der Systemadministrator führt den Installationsassistenten über die Installationsmaschine mit Windows 2008 oder 2012 aus.

- 3 [Prüfen der Voraussetzungen](#) auf Seite 61  
Die Voraussetzungsprüfung stellt sicher, dass Ihre Maschine IaaS-Installationsanforderungen erfüllt.
- 4 [Angaben der Servers und Kontoeinstellungen](#) auf Seite 62  
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](#) auf Seite 63  
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](#) auf Seite 63  
Der Systemadministrator installiert das IaaS-Zertifikat und registriert die IaaS-Komponenten mit SSO.
- 7 [Abschließen der Installation](#) auf Seite 64  
Der Systemadministrator schließt die IaaS-Installation ab.

### Herunterladen des Installationsprogramms für vRealize Automation IaaS

Für die Installation von IaaS auf einem minimalen virtuellen oder physischen Windows-Server laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

### Voraussetzungen

- Microsoft .NET Framework 4.5.2 oder höher. Sie können das .NET-Installationsprogramm von derselben Webseite herunterladen wie das Installationsprogramm für IaaS.
- Achten Sie bei Verwendung von Internet Explorer zum Herunterladen darauf, dass „Verstärkte Sicherheitskonfiguration“ nicht aktiviert ist. Rufen Sie in Internet Explorer `res://iesetup.dll/SoftAdmin.htm` auf dem Windows-Server auf.

### Vorgehensweise

- 1 Melden Sie sich mit einem Konto mit Administratorrechten bei dem Windows-Server an.
- 2 Verweisen Sie in einem Webbrowser auf die folgende URL auf der vRealize Automation-Appliance.  
`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](#)“, auf Seite 81.

### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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“, auf Seite 60.

### Vorgehensweise

- 1 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
<b>Keine Fehler</b>	Klicken Sie auf <b>Weiter</b> .
<b>Nicht kritische Fehler</b>	Klicken Sie auf <b>Umgehung</b> .
<b>Kritische Fehler</b>	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 <b>Erneut prüfen</b> .

- 2 Klicken Sie auf **Weiter**.

Die Maschine erfüllt die Installationsanforderungen.

## Angeben der Servers und Kontoeinstellungen

Der vRealize Automation-Systemadministrator legt Server- und Kontoeinstellungen für den Windows-Installationsserver fest und wählt eine SQL-Datenbank-Server-Instanz sowie eine Authentifizierungsmethode aus.

### Voraussetzungen

„Prüfen der Voraussetzungen“, auf Seite 61.

### Vorgehensweise

- 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 Knowledgebase-Artikel 316898](#).

- 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

„[Angaben der Servers und Kontoeinstellungen](#)“, auf Seite 62.

### Vorgehensweise

- 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](#)“, auf Seite 60.

### Vorgehensweise

- 1 Akzeptieren Sie den **Server**-Standardwert, der mit dem vollqualifizierten Domännennamen des vRealize Automation-Appliance-Servers ausgefüllt wird, von dem Sie den Installer heruntergeladen haben. Stellen Sie sicher, dass ein vollqualifizierter Domänenname zur Identifizierung des Servers und nicht einer IP-Adresse verwendet wird.  
  
Wenn Sie über mehrere virtuelle Appliances verfügen und einen Lastausgleichsdienst verwenden, geben Sie den Pfad der virtuellen Appliance des Lastausgleichsdiensts ein.
- 2 Klicken Sie auf **Laden**, um den Wert für **SSO-Standardmandant** (vsphere.local) auszufüllen.
- 3 Klicken Sie auf **Herunterladen**, um das Zertifikat aus der vRealize Automation-Appliance herunterzuladen.  
  
Zum Anzeigen der Zertifikatsdetails können Sie auf **Zertifikat anzeigen** klicken.
- 4 Wählen Sie **Zertifikat akzeptieren** aus, um das SSO-Zertifikat zu installieren.
- 5 Geben Sie im Feld für den SSO-Administrator **Administrator** in das Textfeld **Benutzername** und das Kennwort ein, das Sie für diesen Benutzer beim Konfigurieren von SSO in **Kennwort** und **Kennwort bestätigen** festgelegt haben.
- 6 Klicken Sie auf den Testlink rechts vom Feld **Benutzername**, um das eingegebene Kennwort zu überprüfen.
- 7 Akzeptieren Sie den Standardwert in **IaaS-Server**, der den Hostnamen der Windows-Maschine enthält, auf der Sie die Installation durchführen.
- 8 Klicken Sie auf den Testlink rechts vom Feld **IaaS-Server**, um die Konnektivität zu überprüfen.

- 9 Klicken Sie auf **Weiter**.

Wenn Sie auf **Weiter** klicken und es wird daraufhin ein Fehler angezeigt, beheben Sie diesen, bevor Sie den Vorgang fortsetzen.

### Abschließen der Installation

Der Systemadministrator schließt die IaaS-Installation ab.

### Voraussetzungen

- „[Registrieren der IaaS-Komponenten](#)“, auf Seite 63.
- Stellen Sie sicher, dass die Maschine, auf der Sie installieren, mit dem Netzwerk verbunden ist und eine Verbindung mit der vRealize Automation-Appliance herstellen kann, von der Sie das IaaS-Installationsprogramm herunterladen.

### Vorgehensweise

- 1 Überprüfen Sie die Informationen auf der Seite Bereit zur Installation und klicken Sie auf **Installieren**.  
Die Installation wird gestartet. In Abhängigkeit von Ihrer Netzwerkkonfiguration kann die Installation zwischen fünf Minuten und einer Stunde dauern.
- 2 Wenn die Erfolgsmeldung angezeigt wird, lassen Sie das Kontrollkästchen **Anweisungen für Erstkonfiguration** aktiviert und klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
- 3 Schließen Sie das Meldungsfeld **System konfigurieren**.

Die Installation ist damit abgeschlossen.

### Weiter

„[Überprüfen der IaaS-Services](#)“, auf Seite 104.

## Verwenden der Standardschnittstellen für verteilte Bereitstellungen

Bei einer verteilten Unternehmensbereitstellung installiert der Systemadministrator Komponenten auf mehreren Maschinen in der Bereitstellungs Umgebung.

### 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 4-2.** Checkliste für die verteilte Bereitstellung

Aufgabe	Details
<input type="checkbox"/> Planen und Vorbereiten der Installationsumgebung und Überprüfen, ob alle Installationsvoraussetzungen erfüllt sind.	<a href="#">Kapitel 2, „Vorbereitung für die Installation von vRealize Automation“</a> , auf Seite 19
<input type="checkbox"/> Planen und Beziehen Ihrer SSL-Zertifikate.	<a href="#">„Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung“</a> , auf Seite 67
<input type="checkbox"/> Bereitstellen des vRealize Automation-Appliance-Hauptservers und zusätzlicher Appliances, die für die Redundanz und High Availability erforderlich sind.	<a href="#">„Bereitstellen der vRealize Automation-Appliance“</a> , auf Seite 70



**Tabelle 4-2.** Checkliste für die verteilte Bereitstellung (Fortsetzung)

Aufgabe	Details
<input type="checkbox"/> Konfigurieren Ihres Lastausgleichsdiensts für die Bewältigung des Datenverkehrs der vRealize Automation-Appliance.	„Konfigurieren des Lastausgleichsdiensts“, auf Seite 72
<input type="checkbox"/> Konfigurieren des vRealize Automation-Appliance-Hauptservers und zusätzlicher Appliances, die Sie für die Redundanz und High Availability bereitgestellt haben.	„Konfigurieren von Appliances für vRealize Automation“, auf Seite 72
<input type="checkbox"/> Konfigurieren Ihres Lastausgleichsdiensts für die Bewältigung des Datenverkehrs der vRealize Automation-IaaS-Komponente und Installieren der vRealize Automation-IaaS-Komponenten.	„Installieren der IaaS-Komponenten in einer verteilten Konfiguration“, auf Seite 79
<input type="checkbox"/> Bei Bedarf Installieren von Agents für die Integration in externe Systeme.	„Installieren der vRealize Automation-Agents“, auf Seite 104
<input type="checkbox"/> Konfigurieren des Standardmandanten und Bereitstellen der IaaS-Lizenz.	„Konfigurieren des Zugriffs auf den Standardmandanten“, auf Seite 129

## 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*.

## Komponenten einer verteilten Installation

Bei einer verteilten Installation stellt der Systemadministrator virtuelle Appliances und zugehörige Komponenten bereit, um die Bereitstellungsumgebung zu unterstützen.

**Tabelle 4-3.** Virtuelle Appliances und Appliance-Datenbank

Komponente	Beschreibung
vRealize Automation-Appliance	Eine vorkonfigurierte virtuelle Appliance, die den vRealize Automation-Server bereitstellt. Zum Server gehört die vRealize Automation-Konsole, die ein zentrales Portal für die Self-Service-Bereitstellung und -Verwaltung von Cloud-Services sowie die Erstellung und Administration darstellt.
Appliance-Datenbank	Speichert für die virtuellen Appliances erforderliche Informationen. Die Datenbank ist in eine oder zwei Instanzen der vRealize Automation-Appliance eingebettet.

Sie können die IaaS-Komponenten auswählen, die Sie installieren möchten, und den Installationsspeicherort angeben.

**Tabelle 4-4.** IaaS-Komponenten

Komponente	Beschreibung
Website	Stellt der vRealize Automation-Konsole die Funktionen für die Infrastrukturadministration und die Erstellung von Diensten zur Verfügung. Die Website-Komponente kommuniziert mit dem Model Manager, von dem sie mit Updates vom Distributed Execution Manager (DEM), von Proxy-Agents und der Datenbank versorgt wird.
Manager Service	Der Manager Service koordiniert die Kommunikation zwischen Agents, der Datenbank, Active Directory und SMTP. Der Manager Service kommuniziert über den Model Manager mit der Konsolenwebsite. Zum Ausführen dieses Diensts sind Administratorrechte erforderlich.
Model Manager	Der Model Manager kommuniziert mit der Datenbank, den DEMs und der Portal-Website. Der Model Manager ist in zwei separat installierbare Komponenten unterteilt, nämlich den Model Manager-Webdienst und die Model Manager-Datenkomponente.
Distributed Execution Manager (Orchestrator und Worker)	Ein Distributed Execution Manager (DEM) führt die Geschäftslogik von benutzerdefinierten Modellen aus und interagiert mit der IaaS-Datenbank und mit externen Datenbanken. DEMs verwalten außerdem Cloud-Maschinen und physische Maschinen.
Agents	Virtualisierungs-, Integrations- und WMI-Agents, die mit Infrastrukturrressourcen kommunizieren.

## Deaktivieren der Integritätsprüfungen des Lastausgleichsdiensts

Mithilfe von Integritätsprüfungen wird sichergestellt, dass ein Lastausgleichsdienst Datenverkehr nur an funktionierende Knoten sendet. Der Lastausgleichsdienst sendet Integritätsprüfungen entsprechend der festgelegten Häufigkeit an jeden Knoten. Knoten, die den Fehlerschwellenwert überschreiten, sind dann nicht mehr zum Empfang von neuen Datenverkehr berechtigt.

Zur Verteilung der Arbeitslast und für Failover können Sie mehrere vRealize Automation-Appliances hinter einem Lastausgleichsdienst platzieren. Außerdem können Sie mehrere IaaS-Webserver sowie mehrere IaaS Manager Service-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 Konfiguration, bevor Sie jegliche Komponenten installieren.
- Nach dem Installieren und Konfigurieren sämtlicher vRealize Automation-Komponenten, einschließlich aller vRealize Automation-Appliance- und IaaS-Komponenten können Sie die Integritätsprüfungen wieder aktivieren.

## Anforderungen an vertrauenswürdige Zertifikate in einer verteilten Bereitstellung

Für die sichere Kommunikation verwendet vRealize Automation Zertifikate, um vertrauenswürdige Beziehungen zwischen Komponenten einzurichten.

Die jeweilige Implementierung der Zertifikate zur Erreichung dieser Vertrauensstellung hängt von Ihrer Umgebung ab.

Zur Unterstützung von High Availability und Failover können Sie Clusterkomponenten mit Lastausgleich bereitstellen. In diesem Fall erhalten Sie ein Mehrfachverwendungszertifikat, das die IaaS Web-Komponente im Cluster enthält, und kopieren anschließend dieses Zertifikat in jede Komponente im Cluster. Sie können Zertifikate mit alternativen Antragstellernamen (Subject Alternative Name, SAN), Platzhalterzertifikate oder eine sonstige für Ihre Umgebung geeignete Methode für die Mehrfachverwendungszertifizierung verwenden, vorausgesetzt, die Anforderungen im Hinblick auf die Vertrauenswürdigkeit sind erfüllt. Wenn Sie Lastausgleichsdienste in Ihrer Bereitstellung verwenden, müssen Sie den FQDN für den Lastausgleichsdienst in der vertrauenswürdigen Adresse des Mehrfachverwendungszertifikats des Clusters angeben.

Beispielsweise können Sie bei einer Lastausgleichsdienstkonfiguration, die ein Zertifikat für den Lastausgleichsdienst sowie für die zugehörigen Komponenten erfordert, ein SAN-Zertifikat zum Zertifizieren von `web-load-balancer.eng.mycompany.com`, `web-component-1.eng.mycompany.com` und `web-component-2.eng.mycompany.com` abrufen. Sie kopieren dann dieses einzelne Mehrfachverwendungszertifikat in den Lastausgleichsdienst und jede Appliance und registrieren anschließend das Zertifikat auf den Webkomponenten-Maschinen.

Die Tabelle „Anforderungen an vertrauenswürdige Zertifikate“ enthält eine Übersicht über die Registrierungsanforderungen der Vertrauensstellung für verschiedene importierte Zertifikate.

**Tabelle 4-5.** Anforderungen an vertrauenswürdige Zertifikate

Importieren	Registrieren
vRealize Automation-Appliance-Cluster	Webkomponentencluster
Webkomponentencluster	<ul style="list-style-type: none"> <li>■ vRealize Automation-Appliance-Cluster</li> <li>■ Manager Service-Komponentencluster</li> <li>■ DEM-Orchestrator- und DEM-Worker-Komponenten</li> </ul>
Manager Service-Komponentencluster	<ul style="list-style-type: none"> <li>■ DEM-Orchestrator- und DEM-Worker-Komponenten</li> <li>■ Agents und Proxy-Agents</li> </ul>

## 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`.

### Vorgehensweise

- 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.

### Weiter

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

Sie können mit diesen Arbeitsblättern wichtige Informationen als Referenz beim Installationsvorgang aufzeichnen.

Eine Kopie eines jeden Arbeitsblatts wird hier bereitgestellt. Erstellen Sie bei Bedarf zusätzliche Kopien. Für die Einstellungen ist die Groß-/Kleinschreibung zu beachten.

**Tabelle 4-6.** Führende Cluster- vRealize Automation-Appliance -Informationen

Variable	Wert	Beispiel
Hostname (FQDN)		vcac-va.mycompany.com
IP		192.168.1.105

**Tabelle 4-6.** Führende Cluster- vRealize Automation-Appliance -Informationen (Fortsetzung)

Variable	Wert	Beispiel
Username	administrator@vsphere.local (Standard)	administrator@vsphere.local
Kennwort		vmware

**Tabelle 4-7.** Zusätzliche vRealize Automation-Appliance -Informationen

Variable	Wert	Beispiel
Hostname (FQDN)		vcac-va2.mycompany.com
IP		192.168.1.110
Username	administrator@vsphere.local (Standard)	administrator@vsphere.local
Kennwort		vmware

**Tabelle 4-8.** Passphrase für IaaS-Datenbank

Variable	Wert	Beispiel
Passphrase (wiederverwendet in IaaS-Installationsprogramm, -Upgrade und -Migration)		myPassphrase

**Tabelle 4-9.** IaaS-Website

Variable	Wert	Beispiel
Hostname (FQDN)		iaas-web.mycompany.com
SSO-Service über ausgehenden HTTPS-Port (Standard)		
IP		192.168.1.106
Username		
Kennwort		

**Tabelle 4-10.** IaaS Model Manager-Daten

Variable	Wert	Beispiel
Hostname (FQDN)		iaas-model-man.mycompany.com
SSO-Service über ausgehenden HTTPS-Port (Standard)		
IP		192.168.1.107
Username		
Kennwort		

**Tabelle 4-11.** IaaS Model-Service

Variable	Wert	Beispiel
Hostname (FQDN)		iaas-model-service.mycompany.com
SSO-Service über ausgehenden HTTPS-Port (Standard)		
IP		192.168.1.108

**Tabelle 4-11.** IaaS Model-Service (Fortsetzung)

Variable	Wert	Beispiel
Username		
Kennwort		

**Tabelle 4-12.** Distributed Execution Manager

Eindeutiger Name	Orchestrator/Worker
zum Beispiel myuniqueorchestratorname	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:

## Bereitstellen der vRealize Automation -Appliance

Für die Bereitstellung der vRealize Automation-Appliance muss sich ein Systemadministrator am vSphere-Client anmelden und Bereitstellungseinstellungen auswählen.

Das Root-Kennwort, das Sie für den vRealize Automation-Administrator erstellen, unterliegt gewissen Einschränkungen.

### Voraussetzungen

- Laden Sie die vRealize Automation-Appliance von der VMware-Website herunter.
- Melden Sie sich bei dem vSphere-Client als ein Benutzer mit Systemadministratorrechten an.

### Vorgehensweise

- 1 Wählen Sie **Datei > OVF-Vorlage bereitstellen** aus dem vSphere-Client aus.
  - 2 Suchen Sie die heruntergeladene vRealize Automation-Appliance-Datei und klicken Sie auf **Öffnen**.
  - 3 Klicken Sie auf **Weiter**.
  - 4 Klicken Sie auf der Seite mit den Einzelheiten zur OVF-Vorlage auf **Weiter**.
  - 5 Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
  - 6 Geben Sie einen eindeutigen Namen für die virtuelle Appliance gemäß der IT-Namenskonvention Ihrer Organisation in das Textfeld **Name** ein, wählen Sie das Datacenter und den Standort aus, für die die virtuelle Appliance bereitgestellt werden soll, und klicken Sie auf **Weiter**.
  - 7 Befolgen Sie die Anleitungen, bis die Seite für das Festplattenformat angezeigt wird.
  - 8 Überprüfen Sie auf der Seite für das Festplattenformat, dass genügend Speicherplatz zum Bereitstellen der virtuellen Appliance vorhanden ist, und klicken Sie auf **Weiter**.
  - 9 Befolgen Sie die Anleitungen, um zur Eigenschaftenseite zu navigieren.
- Die angezeigten Optionen hängen von der vSphere-Konfiguration ab.

- 10 Konfigurieren Sie die Werte auf der Eigenschaftenseite.
  - a Geben Sie das bei der Anmeldung bei der Konsole der virtuellen Appliance zu verwendende Root-Kennwort in die Textfelder **Kennwort eingeben** und **Kennwort bestätigen** ein.
  - b Markieren Sie das Kontrollkästchen **SSH-Dienst** oder heben Sie die Markierung auf, um auszuwählen, ob der SSH-Dienst für die Appliance aktiviert ist.  
  
Dieser Wert wird zum Festlegen des Anfangsstatus des SSH-Diensts in der Appliance verwendet. Wenn Sie den Installationsassistenten für die Installation verwenden, aktivieren Sie diese Option, bevor Sie den Assistenten ausführen. Sie können diese Einstellung nach der Installation über die Appliance-Managementkonsole ändern.
  - c Geben Sie den vollqualifizierten Domännennamen der virtuellen Maschine in das Textfeld **Hostname** ein.
  - d Konfigurieren Sie die Netzwerkeigenschaften.
- 11 Klicken Sie auf **Weiter**.
- 12 Je nach Ihrer Bereitstellungs-, vCenter- und DNS-Konfiguration wählen Sie eines der folgenden Verfahren zum Abschließen der OVA-Bereitstellung und Einschalten der vRealize Automation-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 abgeschlossen ist, klicken Sie auf **Schließen**.
    - c Warten Sie, bis die 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 abgeschlossen ist, klicken Sie auf **Schließen**.
    - b Schalten Sie die vRealize Automation-Appliance ein.
    - c Warten Sie, bis die Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.
    - d Stellen Sie sicher, dass Sie das DNS für die vRealize Automation-Appliance anpingen können. Wenn Sie das DNS nicht anpingen können, starten Sie die virtuelle Maschine neu.
    - e Warten Sie, bis die 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 Maschine gestartet wurde. Dies kann bis zu 5 Minuten dauern.

Wenn Sie überprüfen möchten, ob die Appliance erfolgreich bereitgestellt wurde, öffnen Sie eine Eingabeaufforderung und pingen Sie den FQDN der vRealize Automation-Appliance.

### Weiter

Wiederholen Sie diesen Vorgang, um zusätzliche Instanzen der vRealize Automation-Appliance für die Redundanz in einer High Availability-Umgebung bereitzustellen.

## 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“](#), auf Seite 67. Informationen zum Extrahieren von Zertifikaten finden Sie unter [„Extrahieren von Zertifikaten und privaten Schlüsseln“](#), auf Seite 31.
- 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“](#), auf Seite 72.

---

**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.

---

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 primären vRealize Automation -Appliance

Die vRealize Automation-Appliance ist eine vorkonfigurierte virtuelle Appliance, die den vRealize Automation-Server und die Webkonsole (das Benutzerportal) bereitstellt. Sie wird als Open Virtualization Format (OVF)-Vorlage bereitgestellt. Der Systemadministrator lädt die Appliance herunter und stellt sie in der vCenter Server- oder ESX/ESXi-Bestandsliste bereit.

Wenn Ihr Netzwerk oder Lastausgleichsdienst dies erfordert, wird das Zertifikat, das Sie für die primäre Instanz der Appliance konfigurieren, in den Lastausgleichsdienst und in nachfolgenden Schritten in zusätzliche Appliance-Instanzen kopiert.

### Voraussetzungen

- [„Bereitstellen der vRealize Automation-Appliance“](#), auf Seite 70.



- Rufen Sie ein Domänenzertifikat für die vRealize Automation-Appliance ab.

### Vorgehensweise

- 1 [Aktivieren der Zeitsynchronisierung in der vRealize Automation-Appliance](#) auf Seite 73  
Die Uhren auf dem vRealize Automation-Appliance-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.
- 2 [Konfigurieren der vRealize Automation-Appliance](#) auf Seite 73  
Zur Vorbereitung der vRealize Automation-Appliance für die Verwendung konfiguriert ein Systemadministrator die Hosteinstellungen, generiert ein SSL-Zertifikat und stellt SSO-Verbindungsinformationen bereit.

### Aktivieren der Zeitsynchronisierung in der vRealize Automation-Appliance

Die Uhren auf dem vRealize Automation-Appliance-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 3 Wählen Sie **Administrator > Uhrzeiteinstellungen** aus.
- 4 Wählen Sie eine Option aus dem Menü **Zeitsynchronisierungsmodus** aus.

Option	Aktion
<b>Zeitserver verwenden</b>	Wählen Sie <b>Zeitserver verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um Network Time-Protokoll zu verwenden. Geben Sie für jeden von Ihnen verwendeten Zeitserver die IP-Adresse oder den Hostnamen in das Feld <b>Zeitserver</b> ein.
<b>Hostzeit verwenden</b>	Wählen Sie <b>Hostzeit verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um VMware Tools-Zeitsynchronisierung zu verwenden. Sie müssen die Verbindungen zu NTP-Servern (Network Time Protocol) konfigurieren, bevor Sie die VMware Tools-Zeitsynchronisierung verwenden können.

- 5 Klicken Sie auf **Einstellungen speichern**.
- 6 Überprüfen Sie, dass der Wert in **Aktuelle Uhrzeit** richtig ist.  
Sie können die Zeitzone bei Bedarf auf der Seite für die Zeitzoneneinstellung auf der Registerkarte **System** ändern.

### Konfigurieren der vRealize Automation -Appliance

Zur Vorbereitung der vRealize Automation-Appliance für die Verwendung konfiguriert ein Systemadministrator die Hosteinstellungen, generiert ein SSL-Zertifikat und stellt SSO-Verbindungsinformationen bereit.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Setzen Sie den Vorgang unabhängig von der Zertifikatswarnung fort.

- 3 Melden Sie sich mit dem Benutzernamen „root“ und dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
- 4 Wählen Sie **vRA-Einstellungen > Hosteinstellungen** aus.

Option	Aktion
<b>Automatisch lösen</b>	Wählen Sie <b>Automatisch lösen</b> aus, um den Namen des aktuellen Hosts für die vRealize Automation-Appliance anzugeben.
<b>Host aktualisieren</b>	<p>Wählen Sie für neue Hosts die Option <b>Host aktualisieren</b> aus. Geben Sie den vollqualifizierten Domännennamen der vRealize Automation-Appliance, <i>vra-hostname.domain.name</i>, in das Textfeld <b>Hostname</b> ein.</p> <p>Wählen Sie für verteilte Bereitstellungen mit Lastausgleichsdiensten die Option <b>Host aktualisieren</b> aus. Geben Sie den vollqualifizierten Domännennamen für den Lastausgleichsserver, <i>vra-loadbalancername.domain.name</i>, in das Textfeld <b>Hostname</b> ein.</p>

---

**HINWEIS** Konfigurieren Sie SSO-Einstellungen gemäß der Beschreibung weiter unten in diesem Verfahren immer dann, wenn Sie **Host aktualisieren** zum Festlegen des Hostnamens verwenden.

---

- 5 Wählen Sie aus dem Menü **Zertifikatsaktion** den Zertifikatstyp aus.

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

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

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

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

Option	Aktion
<b>Vorhandene beibehalten</b>	Behalten Sie die aktuelle SSL-Konfiguration bei. Wählen Sie diese Option zum Verwerfen der Änderungen.
<b>Zertifikat generieren</b>	<ul style="list-style-type: none"> <li>a Der im Textfeld <b>Allgemeiner Name</b> 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.</li> <li>b Geben Sie den Namen Ihrer Organisation, wie z. B. den Unternehmensnamen, in das Textfeld <b>Organisation</b> ein.</li> <li>c Geben Sie Ihre Organisationseinheit, wie z. B. den Namen oder den Standort Ihrer Abteilung, in das Textfeld <b>Organisationseinheit</b> ein.</li> <li>d Geben Sie eine zweistellige Landeskennzahl nach ISO 3166 wie z. B. <b>DE</b> in das Textfeld <b>Land</b> ein.</li> </ul>
<b>Importieren</b>	<ul style="list-style-type: none"> <li>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 <b>RSA-Privatschlüssel</b> ein.</li> <li>b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld <b>Zertifikatskette</b> ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu.  <b>HINWEIS</b> Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</li> <li>c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld <b>Passphrase</b> ein.</li> </ul>

- 6 Klicken Sie auf **Einstellungen speichern**, um Hostinformationen und SSL-Konfiguration zu speichern.
- 7 Falls Ihr Netzwerk oder Lastausgleichsdienst dies erfordert, kopieren Sie das importierte oder neu erstellte Zertifikat in den Lastausgleichsdienst der virtuellen Appliance.

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

- a Falls Sie nicht bereits angemeldet sind, melden Sie sich bei der Managementkonsole der vRealize Automation-Appliance als Root-Benutzer an.
- b Klicken Sie auf die Registerkarte **Administrator**.
- c Klicken Sie auf das Untermenü **Administrator**.
- d Aktivieren Sie das Kontrollkästchen **SSH-Dienst aktiviert**.  
  
Deaktivieren Sie das Kontrollkästchen, um SSH nach Abschluss des Vorgangs zu deaktivieren.

- e Aktivieren Sie das Kontrollkästchen **SSH-Anmeldung des Administrators**.  
Deaktivieren Sie das Kontrollkästchen, um SSH nach Abschluss des Vorgangs zu deaktivieren.
  - f Klicken Sie auf **Einstellungen speichern**.
  - 8 Konfigurieren Sie die SSO-Einstellungen.
  - 9 Klicken Sie auf **Dienste**.  
  
Alle Dienste müssen ausgeführt werden, bevor Sie eine Lizenz installieren oder sich bei der Konsole anmelden können. Die Dienste werden in der Regel nach etwa 10 Minuten gestartet.
- 
- HINWEIS** Sie können sich auch bei der Appliance anmelden und `tail -f /var/log/vcac/catalina.out` ausführen, um das Starten der Dienste zu überwachen.
- 
- 10 Geben Sie Ihre Lizenzinformationen ein.
    - a Klicken Sie auf **vRA-Einstellungen > Lizenzierung**.
    - b Klicken Sie auf **Lizenzierung**.
    - c Geben Sie einen gültigen vRealize Automation-Lizenzschlüssel ein, den Sie beim Herunterladen der Installationsdateien heruntergeladen haben, und klicken Sie auf **Schlüssel senden**.
- 
- HINWEIS** Wenn ein Verbindungsfehler auftritt, liegt möglicherweise ein Problem mit dem Lastausgleichsdienst vor. Überprüfen Sie die Netzwerkkonnektivität zum Lastausgleichsdienst.
- 
- 11 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 der vRealize Automation-Konsole anmelden können.
    - a Öffnen Sie einen Browser und navigieren Sie zu `https://vcac-hostname.domain.name/vcac/`.  
Wenn Sie einen Lastausgleichsdienst verwenden, muss der Hostname der vollqualifizierte Domänenname des Lastausgleichsdiensts sein.
    - b Ignorieren Sie ggf. etwaige Zertifikatswarnungen.
    - c Melden Sie sich mit **administrator@vsphere.local** und dem Kennwort an, das Sie bei der Konfiguration von SSO angegeben haben.  
  
Die Konsole wird auf der Seite Mandanten auf der Registerkarte **Administration** geöffnet. Ein einzelner Mandant mit dem Namen `vsphere.local` wird in der Liste angezeigt.

## Konfigurieren zusätzlicher Instanzen der vRealize Automation -Appliance

Der Systemadministrator kann mehrere Instanzen der vRealize Automation-Appliance bereitstellen, um die Redundanz in einer High Availability-Umgebung 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.

### Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance

Die Uhren auf dem vRealize Automation-Appliance-Server und den Windows-Servern müssen synchronisiert werden, um eine erfolgreiche Installation sicherzustellen.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

### Voraussetzungen

„Konfigurieren der primären vRealize Automation-Appliance“, auf Seite 72.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 3 Wählen Sie **Administrator > Uhrzeiteinstellungen** aus.
- 4 Wählen Sie eine Option aus dem Menü **Zeitsynchronisierungsmodus** aus.

Option	Aktion
<b>Zeitserver verwenden</b>	Wählen Sie <b>Zeitserver verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um Network Time-Protokoll zu verwenden. Geben Sie für jeden von Ihnen verwendeten Zeitserver die IP-Adresse oder den Hostnamen in das Feld <b>Zeitserver</b> ein.
<b>Hostzeit verwenden</b>	Wählen Sie <b>Hostzeit verwenden</b> aus dem Menü <b>Zeitsynchronisierungsmodus</b> aus, um VMware Tools-Zeitsynchronisierung zu verwenden. Sie müssen die Verbindungen zu NTP-Servern (Network Time Protocol) konfigurieren, bevor Sie die VMware Tools-Zeitsynchronisierung verwenden können.

- 5 Klicken Sie auf **Einstellungen speichern**.
- 6 Überprüfen Sie, dass der Wert in **Aktuelle Uhrzeit** richtig ist.

Sie können die Zeitzone bei Bedarf auf der Seite für die Zeitzoneneinstellung auf der Registerkarte **System** ändern.

## 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 Verwaltungskonsole der neuen vRealize Automation-Appliance fügen Sie den Knoten einem vorhandenen Cluster aus einer oder mehreren Appliances hinzu. Beim Beitrittsvorgang werden Konfigurationsinformationen auf die von Ihnen hinzugefügte neue Appliance kopiert. Hierzu zählen Zertifikat-, SSO-, Lizenzierungs-, Datenbank- und Messaging-Informationen.

Sie müssen die Appliances einem Cluster nacheinander und nicht parallel hinzufügen.

### Voraussetzungen

- Der Cluster muss bereits einen oder mehrere vRealize Automation-Appliance-Knoten enthalten, wobei ein Knoten der primäre Knoten ist. Siehe „[Konfigurieren der primären vRealize Automation-Appliance](#)“, auf Seite 72.

Ein neuer Knoten kann erst als primärer Knoten festgelegt werden, nachdem Sie den neuen Knoten dem Cluster hinzugefügt haben.

- Stellen Sie sicher, dass der Lastausgleichsdienst für die Verwendung mit der neuen vRealize Automation-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.
- Aktivieren Sie die Uhrzeitsynchronisierung auf dem neuen Knoten. Siehe „[Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance](#)“, auf Seite 77.
- Überprüfen Sie, ob alle vRealize Automation-Dienste auf den vorhandenen Appliance-Knoten des Clusters und auf dem neuen Knoten, den Sie hinzufügen, gestartet wurden.

### Vorgehensweise

- 1 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-va-hostname.domain.name:5480>).
- 2 Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.
- 3 Melden Sie sich mit dem Benutzernamen „root“ und dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.
- 4 Wählen Sie **vRA-Einstellungen > Cluster** aus.
- 5 Geben Sie den FQDN einer zuvor konfigurierten vRealize Automation-Appliance in das Textfeld **Führender Clusterknoten** ein.

Sie können den FQDN der primären vRealize Automation-Appliance oder jeder anderen vRealize Automation-Appliance verwenden, die bereits zum Cluster hinzugefügt wurde.

- 6 Geben Sie das Root-Kennwort in das Textfeld **Kennwort** ein.
- 7 Klicken Sie auf **Cluster beitreten**.
- 8 Setzen Sie den Vorgang unabhängig von Zertifikatswarnungen fort.  
Dienste für das Cluster werden neu gestartet.
- 9 Stellen Sie sicher, dass die Dienste ausgeführt werden.
  - a Klicken Sie auf die Registerkarte **Services**.
  - b Klicken Sie auf die Registerkarte **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

## Deaktivieren nicht verwendeter Dienste

Um interne Ressourcen in Situationen einzusparen, 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](#)“, auf Seite 78

### Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Appliance-Konsole 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 sollten Sie überprüfen, ob Sie auf die Appliances im Cluster zugreifen können.

### Vorgehensweise

- 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 bei der vRealize Automation-Konsole anmelden können, wenn Sie zu <https://vcac-hostname.domain.name/vcac> navigieren, wobei *vcac-hostname.domain.name* die Adresse des Lastausgleichsdiensts darstellt.
- 3 Aktivieren Sie die anderen Knoten wieder, nachdem Sie sichergestellt haben, dass mit dem Lastausgleichsdienst auf die neue vRealize Automation-Appliance zugegriffen werden kann.

## 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 primären vRealize Automation-Appliance](#)“, auf Seite 72.
- Informationen dazu, wenn Ihre Site mehrere Instanzen von vRealize Automation-Appliance enthält, finden Sie unter „[Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster](#)“, auf Seite 78.
- Stellen Sie sicher, dass die Installationsserver die Anforderungen erfüllen, die in „[Anforderungen an den IaaS-Webdienst und den Model Manager-Server](#)“, auf Seite 22 beschrieben sind.
- 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.

## Vorgehensweise

- 1 [Installieren der IaaS-Zertifikate](#) auf Seite 81  
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](#) auf Seite 81  
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](#) auf Seite 82  
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](#) auf Seite 87  
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-Websitekomponenten](#) auf Seite 91  
Die Website-Komponente bietet Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole. Der Systemadministrator kann eine oder viele Instanzen der Website-Komponenten installieren.
- 6 [Installieren der aktiven Manager Service-Komponente](#) auf Seite 94  
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](#) auf Seite 97  
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](#) auf Seite 99  
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](#) auf Seite 102  
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](#) auf Seite 104  
Nach der Installation stellt der Systemadministrator sicher, dass die IaaS-Dienste ausgeführt werden. Wenn die Dienste ausgeführt werden, war die Installation erfolgreich.

## Weiter

Installieren Sie einen DEM-Orchestrator und mindestens eine DEM Worker-Instanz. Siehe „[Installieren von Distributed Execution Managern](#)“, auf Seite 99.



## 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](#).

### Vorgehensweise

- 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.

### Weiter

[„Herunterladen des Installationsprogramms für vRealize Automation IaaS“](#), auf Seite 81.

## Herunterladen des Installationsprogramms für vRealize Automation IaaS

Für die Installation von IaaS auf verteilten virtuellen oder physischen Windows-Servern laden Sie eine Kopie des Installationsprogramms für IaaS von der vRealize Automation-Appliance herunter.

Wenn Zertifikatswarnungen bei diesem Vorgang angezeigt werden, fahren Sie trotzdem mit dem Vorgang fort, um die Installation zu beenden.

### Voraussetzungen

- [„Konfigurieren der primären vRealize Automation-Appliance“](#), auf Seite 72 und optional [„Hinzufügen einer weiteren vRealize Automation-Appliance zum Cluster“](#), auf Seite 78.

- Stellen Sie sicher, dass die Installationsserver die Anforderungen erfüllen, die in „[Anforderungen an den IaaS-Webdienst und den Model Manager-Server](#)“, auf Seite 22 beschrieben sind.
- 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.

### Vorgehensweise

- 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 mit einem Konto mit Administratorrechten bei dem Windows-Server an.
- 3 Verweisen Sie in einem Webbrowser auf die folgende URL auf der vRealize Automation-Appliance.  
<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.

### Weiter

Informationen zum Installieren einer IaaS-Datenbank finden Sie unter „[Auswählen eines IaaS-Datenbankszenarios](#)“, auf Seite 82.

## 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. Informationen zum Konfigurieren von SSL auf dem SQL-Server finden Sie im [Microsoft Knowledgebase-Artikel 316898](#).

---

**Tabelle 4-13.** 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.	„ <a href="#">Manuelles Erstellen der IaaS-Datenbank</a> “, auf Seite 83.
Vorbereiten einer leeren Datenbank und Auffüllen des Datenbankschemas mithilfe des Installationsprogramms. Mithilfe dieser Option kann das Installationsprogramm eine Datenbank mit <b>dbo</b> -Rechten zum Auffüllen der Datenbank verwenden. <b>sysadmin</b> -Rechte sind dann nicht erforderlich.	„ <a href="#">Vorbereiten einer leeren Datenbank</a> “, auf Seite 84.
Erstellen der Datenbank mithilfe des Installationsprogramms. Dies ist die einfachste Option, erfordert jedoch die Verwendung von <b>sysadmin</b> -Rechten für das Installationsprogramm.	„ <a href="#">Erstellen der IaaS-Datenbank mithilfe des Installationsassistenten</a> “, auf Seite 85.

### Manuelles Erstellen der IaaS-Datenbank

Der vRealize Automation-Systemadministrator kann die Datenbank mit von VMware bereitgestellten Skripts manuell erstellen.

#### Voraussetzungen

- Microsoft .NET Framework 4.5.2 oder höher muss auf dem SQL Server-Host installiert sein.
- 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-Datenbankserveranforderungen](#)“, auf Seite 21.
- Laden Sie die Skripts des Installationsprogramms für die IaaS-Datenbank von der vRealize Automation-Appliance unter folgender URL herunter.

<https://vrealize-automation-appliance-FQDN:5480/installer>

#### Vorgehensweise

- 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 4-14.** Datenbankwerte

Variable	Wert
<i>db_server</i>	Gibt die SQL Server-Instanz im Format <code>dbhostname[, port number]\SQL instance</code> an. Geben Sie eine Portnummer nur an, wenn Sie einen nicht standardmäßigen Port verwenden. Die Microsoft SQL-Standardportnummer lautet 1433. Der Standardwert für <i>db_server</i> lautet <code>localhost</code> .
<i>db_name</i>	Der Name der Datenbank. Der Standardwert lautet <code>vra</code> . Datenbanknamen dürfen aus maximal 128 ASCII-Zeichen bestehen.
<i>db_dir</i>	Der Pfad zum Datenverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
<i>log_dir</i>	Der Pfad zum Protokollverzeichnis für die Datenbank, ohne den abschließenden Schrägstrich.
<i>service_user</i>	Der Benutzername, unter dem der Manager Service ausgeführt wird.
<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: <code>6.1.0.1200</code> .

Die Datenbank wird erstellt.

## Weiter

„[Installieren der IaaS-Komponenten in einer verteilten Konfiguration](#)“, auf Seite 79.

## 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-Datenbankserveranforderungen](#)“, auf Seite 21.
- Laden Sie die Skripte des Installationsprogramms für die IaaS-Datenbank von der vRealize Automation-Appliance herunter, indem Sie zu `https://vra-va-hostname.domain.name:5480/installer/` navigieren.

## Vorgehensweise

- 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 `CreateDatabase.sql` und ersetzen Sie alle Instanzen der Variablen in der Tabelle mit den richtigen Werten für Ihre Umgebung.

**Tabelle 4-15. Datenbankwerte**

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

- 5 Prüfen Sie die Einstellungen im Abschnitt **Datenbankeinstellungen** von `CreateDatabase.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 Klicken Sie auf **Ausführen**.  
  
Das Skript wird ausgeführt und erstellt die Datenbank.

**Weiter**

[„Installieren der IaaS-Komponenten in einer verteilten Konfiguration“](#), auf Seite 79.

**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“](#), auf Seite 83.

**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“](#), auf Seite 81.

**Vorgehensweise**

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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 Knowledgebase-Artikel 316898](#).
- 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
<b>Keine Fehler</b>	Klicken Sie auf <b>Weiter</b> .
<b>Nicht kritische Fehler</b>	Klicken Sie auf <b>Umgehung</b> .
<b>Kritische Fehler</b>	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 <b>Erneut prüfen</b> .

- 18 Klicken Sie auf **Installieren**.
- 19 Wenn die Erfolgsmeldung angezeigt wird, deaktivieren Sie **Anweisungen für Erstkonfiguration** und klicken Sie auf **Weiter**.
- 20 Klicken Sie auf **Beenden**.

Die Datenbank ist einsatzbereit.

## Installieren von IaaS-Website-Komponente und Model Manager-Daten

Der Systemadministrator installiert die Website-Komponente, um Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole bereitzustellen. Sie können eine oder viele Instanzen der Website-Komponente installieren, aber Sie müssen Model Manager-Daten auf der Maschine konfigurieren, die die erste Website-Komponente hostet. Sie installieren Model Manager-Daten nur einmal.

### Voraussetzungen

- Informationen zum Installieren der IaaS-Datenbank finden Sie unter [„Auswählen eines IaaS-Datenbankszenarios“](#), auf Seite 82.
- Wenn Sie zuvor andere Komponenten in dieser Umgebung installiert haben, stellen Sie sicher, dass Sie die erstellte Passphrase kennen. Siehe [„Sicherheitskennwortsatz“](#), auf Seite 31.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

## Vorgehensweise

- 1 [Installieren der ersten IaaS-Website-Komponente](#) auf Seite 88  
Ein Systemadministrator installiert die Website-Komponente, um Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole bereitzustellen.
- 2 [Konfigurieren von Model Manager Data](#) auf Seite 90  
Die Model Manager-Komponente installieren Sie auf derselben Maschine, auf der auch die erste Website-Komponente gehostet wird. Model Manager-Daten können nur einmal installiert werden.

Sie können zusätzliche Website-Komponenten oder den Manager Service installieren. Siehe [„Installieren zusätzlicher IaaS-Websitekomponenten“](#), auf Seite 91 oder [„Installieren der aktiven Manager Service-Komponente“](#), auf Seite 94.

## Installieren der ersten IaaS-Website-Komponente

Ein Systemadministrator installiert die Website-Komponente, um Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole bereitzustellen.

Sie können mehrere Website-Komponenten installieren; es darf jedoch nur eine davon Model Manager-Daten enthalten. Model Manager-Daten müssen auf der ersten erstellten Website-Komponente installiert werden.

## Voraussetzungen

- [„Erstellen der IaaS-Datenbank mithilfe des Installationsassistenten“](#), auf Seite 85.
- Stellen Sie sicher, dass die Umgebung die Anforderungen erfüllt, die in [„Anforderungen an den IaaS-Webdienst und den Model Manager-Server“](#), auf Seite 22 beschrieben sind.
- Wenn Sie zuvor andere Komponenten in dieser Umgebung installiert haben, stellen Sie sicher, dass Sie die erstellte Passphrase kennen. Siehe [„Sicherheitskennwortsatz“](#), auf Seite 31.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

## Vorgehensweise

- 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__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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-Zertifikatsperrlisten.  
Diese Option ist weniger sicher.

## Konfigurieren von Model Manager Data

Die Model Manager-Komponente installieren Sie auf derselben Maschine, auf der auch die erste Website-Komponente gehostet wird. Model Manager-Daten können nur einmal installiert werden.

### Voraussetzungen

„[Installieren der ersten IaaS-Website-Komponente](#)“, auf Seite 88.

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Model Manager-Daten**.
- 2 Geben Sie den vollqualifizierten Domännennamen der vRealize Automation-Appliance in das Textfeld **Server** ein.  
  
IP-Adressen werden nicht erkannt.  
  
Beispielsweise **vra.mycompany.com**.
- 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 Geben Sie in das Textfeld **IaaS-Server** den vollqualifizierten Namen des IaaS Website-Servers ein.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des Lastausgleichs-diensts für den IaaS Website-Server ein. Beispielsweise <b>IaaS-load-balancer.eng.mycompany.com</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des IaaS Website-Servers ein. Beispielsweise <b>IaaS.eng.mycompany.com</b> . IP-Adressen werden nicht erkannt.

- 10 Klicken Sie auf **Testen**, um die Serververbindung zu überprüfen.
- 11 Klicken Sie auf **Weiter**.
- 12 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
<b>Keine Fehler</b>	Klicken Sie auf <b>Weiter</b> .
<b>Nicht kritische Fehler</b>	Klicken Sie auf <b>Umgehung</b> .
<b>Kritische Fehler</b>	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 <b>Erneut prüfen</b> .

- 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
<b>Wenn Sie bereits Komponenten in dieser Umgebung installiert haben</b>	Geben Sie die zuvor erstellte Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein.
<b>Wenn dies die erste Installation ist</b>	Geben Sie eine Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

- 15 Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.

Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.

- 16 Klicken Sie auf **Weiter**.

- 17 Klicken Sie auf **Installieren**.

- 18 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.

## Weiter

Sie können zusätzliche Website-Komponenten oder den Manager Service installieren. Siehe „[Installieren zusätzlicher IaaS-Websitekomponenten](#)“, auf Seite 91 oder „[Installieren der aktiven Manager Service-Komponente](#)“, auf Seite 94.

## Installieren zusätzlicher IaaS-Websitekomponenten

Die Website-Komponente bietet Zugriff auf Infrastrukturfunktionen in der vRealize Automation-Webkonsole. Der Systemadministrator kann eine oder viele Instanzen der Website-Komponenten installieren.

Installieren Sie keine Model Manager-Daten mit der Website-Komponente. Nur die erste Website-Komponente, die Sie installieren, kann Model Manager-Daten enthalten.

## Voraussetzungen

- „[Installieren von IaaS-Website-Komponente und Model Manager-Daten](#)“, auf Seite 87.
- Stellen Sie sicher, dass die Umgebung die Anforderungen erfüllt, die in „[Anforderungen an den IaaS-Webdienst und den Model Manager-Server](#)“, auf Seite 22 beschrieben sind.
- Wenn Sie zuvor andere Komponenten in dieser Umgebung installiert haben, stellen Sie sicher, dass Sie die erstellte Passphrase kennen. Siehe „[Sicherheitskennwortsatz](#)“, auf Seite 31.
- Wenn Sie Lastausgleichsmodule in der Umgebung verwenden, stellen Sie sicher, dass sie die Konfigurationsanforderungen erfüllen.

## Vorgehensweise

- 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__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 10 Klicken Sie auf **Weiter**.
- 11 Wählen Sie **Website** auf der Seite Benutzerdefinierte Installation des IaaS-Servers aus.
- 12 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.
- 13 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.
- 14 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.

- 15 Wählen Sie das Zertifikat für diese Komponente aus.
- a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
  - b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
  - c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen. Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom IaaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

- 16 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 17 (Optional) Wählen Sie **Zertifikatkonflikt unterdrücken** aus, um Zertifikatfehler zu unterdrücken. Die Installation ignoriert Fehler bei Zertifikatnamenskonflikten sowie Fehler bei Konflikten mit Remote-Zertifikatsperrlisten.

Diese Option ist weniger sicher.

- 18 Geben Sie die IaaS-Serverinformationen in das Textfeld **IaaS-Server** ein.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des Lastausgleichsdiensts für den IaaS Website-Server ein. Beispielsweise <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des IaaS Website-Servers ein. Beispielsweise <b>IaaS.eng.mycompany.com</b> .

- 19 Klicken Sie auf **Testen**, um die Serververbindung zu überprüfen.
- 20 Klicken Sie auf **Weiter**.
- 21 Schließen Sie die Voraussetzungsprüfung ab.

Option	Beschreibung
<b>Keine Fehler</b>	Klicken Sie auf <b>Weiter</b> .
<b>Nicht kritische Fehler</b>	Klicken Sie auf <b>Umgehung</b> .
<b>Kritische Fehler</b>	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 <b>Erneut prüfen</b> .

- 22 Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

- 23 Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
<b>Wenn Sie bereits Komponenten in dieser Umgebung installiert haben</b>	Geben Sie die zuvor erstellte Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein.
<b>Wenn dies die erste Installation ist</b>	Geben Sie eine Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> 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**.

#### Weiter

[„Installieren der aktiven Manager Service-Komponente“](#), auf Seite 94.

## 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.

Für Ihre IaaS-Bereitstellung ist es erforderlich, dass der Manager Service nur auf einer Windows-Maschine aktiv ausgeführt wird. Für Backups oder Hochverfügbarkeit können Sie zusätzliche Windows-Maschinen bereitstellen, auf denen Sie den Manager Service manuell starten, falls der aktive Dienst beendet wird.

**WICHTIG** Die gleichzeitige Ausführung eines aktiven Manager Service auf mehreren IaaS-Windows-Servern hat zur Folge, dass vRealize Automation nicht verwendet werden kann.

#### Voraussetzungen

- Wenn Sie zuvor andere Komponenten in dieser Umgebung installiert haben, stellen Sie sicher, dass Sie die erstellte Passphrase kennen. Siehe [„Sicherheitskennwortsatz“](#), auf Seite 31.
- (Optional) Wenn Sie den Manager Service in einer anderen Website als die Standardwebsite installieren möchten, erstellen Sie zuerst eine Website in den Internetinformationsdiensten.
- Microsoft .NET Framework 4.5.2 ist installiert.
- 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“](#), auf Seite 87.

## Vorgehensweise

- 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__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 9 Klicken Sie auf **Weiter**.
- 10 Wählen Sie **Manager Service** auf der Seite Benutzerdefinierte Installation des IaaS-Servers aus.
- 11 Geben Sie die IaaS-Serverinformationen in das Textfeld **IaaS-Server** ein.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des Lastausgleichsdiensts für den IaaS Website-Server ein. Beispielsweise <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des IaaS Website-Servers ein. Beispielsweise <b>IaaS.eng.mycompany.com</b> .

- 12 Wählen Sie **Aktiver Knoten mit Starttyp Automatisch** aus.
- 13 Wählen Sie eine Website aus den verfügbaren Websites aus oder akzeptieren Sie die Standardwebsite auf der Registerkarte **Verwaltung und Model Manager-Website**.
- 14 Geben Sie eine verfügbare Portnummer in das Textfeld **Portnummer** ein oder akzeptieren Sie den Standardport 443.
- 15 Klicken Sie auf **Test Binding**, um zu bestätigen, dass die Portnummer für die Verwendung verfügbar ist.

- 16 Wählen Sie das Zertifikat für diese Komponente aus.
  - a Wenn Sie ein Zertifikat nach Start der Installation importiert haben, klicken Sie zum Aktualisieren der Liste auf **Aktualisieren**.
  - b Wählen Sie das zu verwendende Zertifikat aus **Verfügbare Zertifikate** aus.
  - c Wenn Sie ein Zertifikat ohne Anzeigenamen importiert haben und dieses nicht in der Liste angezeigt wird, heben Sie die Auswahl von **Zertifikate unter Verwendung von Anzeigenamen anzeigen** auf und klicken Sie auf **Aktualisieren**.

Wenn Sie in einer Umgebung installieren, in der keine Lastausgleichsmodule verwendet werden, können Sie **Ein selbstsigniertes Zertifikat erstellen** auswählen, anstatt ein Zertifikat auszuwählen. Wenn Sie zusätzliche Websitekomponenten hinter einem Lastausgleichsdienst installieren, erstellen Sie keine selbstsignierten Zertifikate. Importieren Sie das Zertifikat vom IaaS-Hauptwebserver, um sicherzustellen, dass Sie dasselbe Zertifikat auf allen Servern hinter dem Lastausgleichsdienst verwenden.

- 17 (Optional) Klicken Sie auf **Zertifikat anzeigen**, zeigen Sie das Zertifikat an und klicken Sie zum Schließen des Informationsfensters auf **OK**.
- 18 Klicken Sie auf **Weiter**.
- 19 Überprüfen Sie die Voraussetzungen und klicken Sie auf **Weiter**.
- 20 Geben Sie auf der Seite „Server- und Kontoeinstellungen“ in den Textfeldern unter **Informationen zur Serverinstallation** den Benutzernamen und das Kennwort des Dienstkontobenutzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.

Bei dem Dienstkontobenutzer muss es sich um ein Domänenkonto handeln, das über Rechte für jeden verteilten IaaS-Server verfügt. Verwenden Sie keine lokalen Systemkonten.

- 21 Geben Sie die Passphrase ein, die zum Erstellen des Verschlüsselungsschlüssels für den Schutz der Datenbank verwendet wurde.

Option	Beschreibung
<b>Wenn Sie bereits Komponenten in dieser Umgebung installiert haben</b>	Geben Sie die zuvor erstellte Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein.
<b>Wenn dies die erste Installation ist</b>	Geben Sie eine Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> 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**.

## Weiter

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](#)“, auf Seite 97.

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](#)“, auf Seite 102.

## 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.

Für Ihre IaaS-Bereitstellung ist es erforderlich, dass der Manager Service nur auf einer Windows-Maschine aktiv ausgeführt wird. Auf Maschinen, auf denen der Manager Service für Backups verfügbar ist, muss der Dienst beendet und für den manuellen Start konfiguriert werden.

---

**WICHTIG** Die gleichzeitige Ausführung eines aktiven Manager Service auf mehreren IaaS-Windows-Servern hat zur Folge, dass vRealize Automation nicht verwendet werden kann.

---

### Voraussetzungen

- Wenn Sie zuvor andere Komponenten in dieser Umgebung installiert haben, stellen Sie sicher, dass Sie die erstellte Passphrase kennen. Siehe „[Sicherheitskennwortsatz](#)“, auf Seite 31.
- (Optional) Wenn Sie den Manager Service in einer anderen Website als die Standardwebsite installieren möchten, erstellen Sie zuerst eine Website in den Internetinformationsdiensten.
- Microsoft .NET Framework 4.5.2 ist installiert.
- 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](#)“, auf Seite 87.

### Vorgehensweise

- 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__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 10 Klicken Sie auf **Weiter**.
- 11 Wählen Sie **Manager Service** auf der Seite Benutzerdefinierte Installation des IaaS-Servers aus.
- 12 Geben Sie die IaaS-Serverinformationen in das Textfeld **IaaS-Server** ein.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des Lastausgleichsdiensts für den IaaS Website-Server ein. Beispielsweise <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen des IaaS Website-Servers ein. Beispielsweise <b>IaaS.eng.mycompany.com</b> .

- 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 Dienstkotobenzers ein, der Administratorrechte für den aktuellen Installationsserver aufweist.  
  
Bei dem Dienstkotobenzers 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
<b>Wenn Sie bereits Komponenten in dieser Umgebung installiert haben</b>	Geben Sie die zuvor erstellte Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein.
<b>Wenn dies die erste Installation ist</b>	Geben Sie eine Passphrase in die Textfelder <b>Passphrase</b> und <b>Bestätigen</b> ein. Sie müssen diese Passphrase jedes Mal verwenden, wenn Sie eine neue Komponente installieren.

Bewahren Sie diese Passphrase an einem sicheren Ort für die spätere Verwendung auf.

- 23 Geben Sie den IaaS-Datenbankserver, den Datenbanknamen und die Authentifikationsmethode für den Datenbankserver im das Textfeld **Installationsinformationen für Microsoft SQL-Datenbank** ein.  
  
Dies sind der IaaS-Datenbankserver, der Name und die Authentifizierungsinformationen, die Sie zuvor erstellt haben.
- 24 Klicken Sie auf **Weiter**.
- 25 Klicken Sie auf **Installieren**.
- 26 Wenn die Installation beendet wird, heben Sie die Auswahl von **Führen Sie mich durch die Erstkonfiguration** auf und klicken Sie auf **Weiter**.
- 27 Klicken Sie auf **Beenden**.

## Weiter

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“](#), auf Seite 102.

## 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 „[Anforderungen an den Distributed Execution Manager](#)“, auf Seite 23.

### Installieren der Distributed Execution Manager

Ein Systemadministrator installiert mindestens einen DEM-Worker und einen DEM-Orchestrator. 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](#)“, auf Seite 81.

### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.

- 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
<b>Worker</b>	Der Worker führt Workflows aus.
<b>Orchestrator</b>	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.  
Wenn Sie das Migrationstool verwenden möchten, muss dieser Name genau mit dem in der vCloud Automation Center 5.2.3-Installation verwendeten Namen übereinstimmen. 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
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie die vollqualifizierten Domännennamen der Lastausgleichsmodule für den Manager Service und den Model Manager-Webdienst ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> and <b>web-load-balancer.eng.mycompany.com:443</b> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie die vollqualifizierten Domännennamen von Manager Service und des Model Manager-Webdiensts ein. Beispielsweise <b>manager-service.eng.mycompany.com:443</b> and <b>model-manager.eng.mycompany.com:443</b> .

- 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**.

## Weiter

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 der Verbindungsherstellung des DEM mit SCVMM über einen nicht standardmäßigen Installationspfad

Standardmäßig verweist die DEM-Worker-Konfigurationsdatei (DynamicOps.DEM.exe.config) auf den Standardinstallationspfad der System Center Virtual Machine Manager (SCVMM)-Konsole von Microsoft: {Programme}\Microsoft System Center 2012\Virtual Machine Manager\bin. Der Systemadministrator muss den Pfad ändern, wenn sie in einem anderen Speicherort installiert wurde.

Dieser Schritt ist nur erforderlich, wenn SCVMM-Endpoints und -Agents vorhanden sind.

## Voraussetzungen

- Wenn die SCVMM-Konsole in einem anderen Speicherort installiert wurde, muss die DEM-Worker-Konfigurationsdatei (im Verzeichnis Programme (x86)\VMware\VCAC\Distributed Execution Manager\<Instanzname>\DynamicOps.DEM.exe.config) aktualisiert werden, um den Standardpfad im Abschnitt `assemblyLoadConfiguration` zu ändern, sodass er auf den neuen Ordner verweist.

```
<assemblyLoadConfiguration>
    <assemblies>
        <!-- List of required assemblies for Scvmm -->
        <add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012\Virtual
            Machine Manager\bin" />
        [...]
    </assemblies>
</assemblyLoadConfiguration>
```

## Vorgehensweise

- 1 Beenden Sie den DEM-Worker.
- 2 Bestimmen Sie den Installationspfad.
- 3 Aktualisieren Sie die Datei DynamicOps.DEM.exe.config.
- 4 Starten Sie den DEM-Worker neu.

Der DEM-Worker-Standardpfad wird auf den neuen Ordner aktualisiert.

## 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“, auf Seite 82.
- Stellen Sie sicher, dass der Benutzername, unter dem der Manager Service ausgeführt werden soll, nicht der Besitzer der Datenbank ist.

#### Vorgehensweise

- 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**.

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“, auf Seite 82.

#### Vorgehensweise

- 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.

### Vorgehensweise

- 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“](#), auf Seite 107.

## 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 TechNet-Artikel hh847748](#). Wenn Ihre PowerShell-Ausführungsrichtlinie auf der Gruppenrichtlinienebene verwaltet wird, wenden Sie sich an Ihren IT-Support, um Informationen zu den geltenden Einschränkungen bei Richtlinienänderungen zu erhalten, und lesen Sie im [Microsoft TechNet-Artikel jj149004](#) nach.

### Voraussetzungen

- Melden Sie sich als Windows-Administrator an.
- 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.

### Vorgehensweise

- 1 Wählen Sie **Start > Alle Programme > Windows PowerShell-Version > Windows PowerShell**.
- 2 Führen Sie für „Remote signiert“ `Set-ExecutionPolicy RemoteSigned` aus.
- 3 Führen Sie für „Nicht eingeschränkt“ `Set-ExecutionPolicy Unrestricted` aus.
- 4 Prüfen Sie, ob der Befehl zu keinerlei Fehlern geführt hat.
- 5 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 4-16.** 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“, auf Seite 106
Bereitstellung virtueller Maschinen durch die Integration in eine Microsoft Hyper-V Server-Umgebung.	„Installieren des Proxy-Agents für Hyper-V oder XenServer“, auf Seite 112
Bereitstellung virtueller Maschinen durch die Integration in eine XenServer-Umgebung.	<ul style="list-style-type: none"> <li>■ „Installieren des Proxy-Agents für Hyper-V oder XenServer“, auf Seite 112</li> <li>■ „Installieren des EPI-Agents für Citrix“, auf Seite 119</li> </ul>
Bereitstellung virtueller Maschinen durch die Integration in eine XenDesktop-Umgebung.	<ul style="list-style-type: none"> <li>■ „Installieren des VDI-Agents für XenDesktop“, auf Seite 116</li> <li>■ „Installieren des EPI-Agents für Citrix“, auf Seite 119</li> </ul>
Ausführung von Visual Basic-Skripts als zusätzliche Schritte im Bereitstellungsprozess vor oder nach der Bereitstellung einer Maschine oder während der Aufhebung der Bereitstellung.	„Installieren des EPI-Agents für Visual Basic-Skripterstellung“, auf Seite 122
Erfassen von Daten von den bereitgestellten Windows-Maschinen, beispielsweise der Active Directory-Status des Besitzers einer Maschine.	„Installieren des WMI-Agents für WMI-Remoteanforderungen“, auf Seite 125
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.

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 4-17.** Erforderliche Berechtigungen an vSphere -Agents für die Verwaltung von vCenter Server - Instanzen

Attributwert		Berechtigung
Datenspeicher		Speicher zuteilen
		Datenspeicher durchsuchen
Datenspeicher-Cluster		Konfigurieren eines Datenspeicher-Clusters
Ordner		Ordner erstellen
		Ordner löschen
Global		Benutzerdefinierte Attribute verwalten
		Benutzerdefiniertes Attribut festlegen
Netzwerk		Netzwerk zuweisen
Berechtigungen		Berechtigung ändern
Ressourcen		Ressourcenpool VMs zuweisen
		Ausgeschaltete virtuelle Maschine migrieren
		Eingeschaltete virtuelle Maschine migrieren
Virtuelle Maschine	Bestandsliste	Aus vorhandener erstellen
		Neue erstellen
		Verschieben
		Entfernen
	Interaktion	CD-Medien konfigurieren
		Konsoleninteraktion
		Geräteverbindung
		Ausschalten
		Einschalten
		Zurücksetzen
		Anhalten
		Tools installieren
	Konfiguration	Vorhandene Festplatte hinzufügen

**Tabelle 4-17.** Erforderliche Berechtigungen an vSphere -Agents für die Verwaltung von vCenter Server - Instanzen (Fortsetzung)

Attributwert	Berechtigung
	Neue Festplatte hinzufügen
	Hinzufügen oder entfernen
	Festplatte entfernen
	Erweitert
	CPU-Anzahl ändern
	Ressourcen ändern
	Virtuelle Festplatte erweitern
	Festplattenänderungsverfolgung
	Arbeitsspeicher
	Geräteeinstellungen ändern
	Umbenennen
	Anmerkung festlegen (Version 5.0 und höher)
	Einstellungen
Bereitstellung	Platzierung der Auslagerungsdatei
	Anpassen
	Vorlage klonen
	Virtuelle Maschine klonen
	Vorlage bereitstellen
Zustand	Anpassungsspezifikationen lesen
	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

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- Stellen Sie sicher, dass Sie alle „[vSphere Agent-Anforderungen](#)“, auf Seite 107 erfüllen.
- 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](#)“, auf Seite 81.

## Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

---

- 13 Konfigurieren Sie eine Verbindung zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 14 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.

## Weiter

„Konfigurieren des vSphere-Agents“, auf Seite 111.

## Konfigurieren des vSphere -Agents

Sie können das Proxy-Agent-Dienstprogramm verwenden, um die Erstkonfigurationen zu bearbeiten, die in der Agent-Konfigurationsdatei `VRMAgent.exe.config` verschlüsselt sind, oder um die Maschinen-Löschrichtlinie für Virtualisierungsplattformen zu ändern.

Konfigurieren Sie den vSphere-Agenten als Vorbereitung für die Erstellung und Verwendung von vSphere-Endpoints, die in vRealize Automation-Blueprints eingesetzt werden sollen.

---

**HINWEIS** Bestimmte Teile der Datei sind verschlüsselt, andere hingegen nicht. Der Abschnitt „serviceConfiguration“ der Datei `VRMAgent.exe.config` ist beispielsweise nicht verschlüsselt.

---

### Voraussetzungen

Melden Sie sich als **Systemadministrator** an der Maschine an, auf der Sie den vSphere-Agenten installiert haben.

### Vorgehensweise

- 1 Öffnen Sie als Administrator eine Windows-Befehlskonsole.
- 2 Navigieren Sie zum Agent-Installationsverzeichnis.  
Beispiel: `cd Program Files (x86)\VMware\VCAC\CD Agents\agent_name.`
- 3 (Optional) Geben Sie `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` ein, um die aktuellen Konfigurationseinstellungen anzuzeigen.  
Nachfolgend finden Sie ein Beispiel für die Befehlsausgabe:  
`managementEndpointName: VCEndpoint doDeletes: True`
- 4 (Optional) Geben Sie den Befehl `set managementEndpointName` ein, um den Namen des bei der Installation konfigurierten Endpoints zu ändern.  
Beispiel: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName MeinEndpoint.`  
Sie bearbeiten diese Eigenschaft zum Umbenennen des Endpoints innerhalb von vRealize Automation, anstatt Endpoints zu ändern.
- 5 (Optional) Geben Sie den Befehl `set doDeletes` ein, um die Löschrichtlinie der virtuellen Maschine zu konfigurieren.  
Beispiel: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false.`

Option	Beschreibung
<b>Wahr</b>	(Standard) Löschen Sie die von vCenter Server in vRealize Automation gelöschten virtuellen Maschinen.
<b>Falsch</b>	Verschieben Sie virtuelle Maschinen, die in vRealize Automation gelöscht wurden, ins Verzeichnis <code>VRMDeleted</code> in vCenter Server.

- 6 (Optional) Fordern Sie ein vertrauenswürdiges Zertifikat für den vSphere-Agenten an, indem Sie den Parameter `trustAllCertificates` mithilfe der folgenden Anweisung im Abschnitt `serviceConfiguration` der Datei `VRMAgent.exe.config` auf „False“ festlegen:

```
trustAllCertificates = "false"
```

Da diese Einstellung nicht verschlüsselt ist, können Sie den Befehl `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set trustAllCertificates false` nicht verwenden.

Option	Beschreibung
<b>Wahr</b>	(Standard) Der vSphere-Agent benötigt kein vertrauenswürdiges Zertifikat vom vCenter Server.
<b>Falsch</b>	Der vSphere-Agent benötigt ein vertrauenswürdiges Zertifikat vom vCenter Server.

- 7 Navigieren Sie zu **Start > Verwaltung > Dienste** und starten Sie den Dienst vRealize Automation-Agent – *Agent\_Name* neu.

### Weiter

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 Domännennamen identifiziert werden.

**HINWEIS** Standardmäßig ist Hyper-V nicht für die Remoteverwaltung konfiguriert. Ein vRealize Automation Hyper-V-Proxy-Agent kann nur mit einem Hyper-V-Server kommunizieren, wenn die Remoteverwaltung aktiviert wurde.

Informationen zum Konfigurieren von Hyper-V für die Remoteverwaltung finden Sie in der Dokumentation zu Microsoft Windows Server.

## Installieren des Hyper-V- oder XenServer-Agents

Der Hyper-V-Agent verwaltet Hyper-V-Server-Instanzen. Der XenServer-Agent verwaltet XenServer-Server-Instanzen.

### Voraussetzungen

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- [„Herunterladen des Installationsprogramms für vRealize Automation IaaS“](#), auf Seite 81.



- 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 Automation Hyper-V-Proxy-Agents zu aktivieren.

Informationen zum Konfigurieren von Hyper-V für die Remoteverwaltung finden Sie in der Dokumentation zu Microsoft Windows Server.

### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

- 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 zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 15 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.

### Weiter

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“](#), auf Seite 115.

## Konfigurieren des Hyper-V - oder XenServer -Agents

Der Systemadministrator kann die Konfigurationseinstellungen für den Proxy-Agent ändern, wie beispielsweise die Löschrichtlinie 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.

### Vorgehensweise

- 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
```

### Weiter

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 Xen-Server-Hostnamens](#)“, auf Seite 117.

Jeder XenDesktop DDC-Server, mit dem Sie Maschinen registrieren möchten, muss folgendermaßen konfiguriert werden:

- Der Gruppen- bzw. Katalogtyp muss zur Verwendung mit vRealize Automation auf **Vorhanden** festgelegt sein.
- Der Name eines vCenter Server-Hosts auf einem DDC-Server muss mit dem Namen auf der vCenter Server-Instanz übereinstimmen, wie er auf dem vRealize Automation vSphere-Endpoint eingegeben wurde (ohne Domäne). Der Endpoint muss mit einem vollqualifizierten Domännennamen (FQDN), nicht jedoch mit einer IP-Adresse, konfiguriert werden. Wenn die Adresse auf dem Endpoint z. B. „https://virtual-center27.domain/sdk“ lautet, muss der Name des Hosts auf dem DDC-Server auf „virtual-center27“ festgelegt werden.

Wenn Ihr vRealize Automation vSphere-Endpoint mit einer IP-Adresse konfiguriert wurde, müssen Sie dies ändern und einen FQDN verwenden. Weitere Informationen zum Einrichten von Endpoints finden Sie unter *IaaS-Konfiguration*.

### Anforderungen an XenDesktop-Agent-Host

Citrix XenDesktop SDK muss installiert sein. Das SDK für XenDesktop ist auf XenDesktop-Installationsmedium enthalten.

Stellen Sie vor der Agent-Installation sicher, dass Microsoft PowerShell auf dem Installationshost installiert ist. Die erforderliche Version hängt vom Betriebssystem des Installationshosts ab. Informieren Sie sich unter „Hilfe und Support“ von Microsoft.

Die MS PowerShell-Ausführungsrichtlinie ist auf RemoteSigned oder Unrestricted festgelegt. Siehe „[Festlegen der PowerShell-Ausführungsrichtlinie auf RemoteSigned](#)“, auf Seite 105.

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.

#### Vorgehensweise

- 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

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- Stellen Sie sicher, dass die Umgebung die „[XenDesktop-Anforderungen](#)“, auf Seite 116 erfüllt.
- „[Herunterladen des Installationsprogramms für vRealize Automation IaaS](#)“, auf Seite 81.

#### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

- 14 Konfigurieren Sie eine Verbindung zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 15 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.

### Weiter

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](#)“, auf Seite 120 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](#)“, auf Seite 105.

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

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- Stellen Sie sicher, dass Sie alle „[Anforderungen an Citrix Provisioning Server](#)“, auf Seite 119 erfüllen.
- „[Herunterladen des Installationsprogramms für vRealize Automation IaaS](#)“, auf Seite 81.

#### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

- 13 Konfigurieren Sie eine Verbindung zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 14 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.

#### Weiter

Für High Availability können Sie einen redundanten Agent für den Endpoint installieren und konfigurieren. Installieren Sie jeden redundanten Agent auf einem separaten Server, aber benennen und konfigurieren Sie die Agents gleich.

## Installieren des EPI-Agents für Visual Basic-Skripterstellung

Ein Systemadministrator kann Visual Basic-Skripts als zusätzliche Schritte im Bereitstellungsvorgang angeben. Dies kann vor, während oder nach der Bereitstellung einer Maschine erfolgen. Sie müssen vor dem Ausführen von Visual Basic-Skripts einen EPI-PowerShell-Agent (External Provisioning Integration) installieren.

Visual Basic-Skripts werden in dem Blueprint angegeben, von dem aus Maschinen bereitgestellt werden. Diese Skripts haben Zugriff auf alle benutzerdefinierten Eigenschaften, die mit den Maschinen verknüpft sind, und können deren Werte aktualisieren. Der nächste Schritt in dem Workflow hat Zugriff auf diese neuen Werte.

Sie können beispielsweise mit einem Skript Zertifikate oder Sicherheitstoken vor der Bereitstellung erstellen und diese bei der Maschinenbereitstellung verwenden.

Um Skripts in der Bereitstellung zu aktivieren, müssen Sie einen bestimmten Typ eines EPI-Agents installieren und die zu verwendenden Skripts auf dem System positionieren, auf dem der Agent installiert ist.

Bei der Ausführung eines Skripts leitet der EPI-Agent alle benutzerdefinierten Eigenschaften der Maschine als Argumente an das Skript weiter. Um aktualisierte Eigenschaftswerte zurückzugeben, müssen Sie diese Eigenschaften in einem Wörterbuch positionieren und eine vRealize Automation-Funktion aufrufen. Ein Beispielskript ist im Unterverzeichnis des Installationsverzeichnisses des EPI-Agents des Skripts enthalten. Dieses Skript enthält eine Überschrift zum Laden aller Argumente in ein Wörterbuch, einen Text, in den Sie die Funktion(en) hinzufügen können, und eine Fußzeile zum Zurückgeben der benutzerdefinierten Eigenschaftswerte.

**HINWEIS** Sie können mehrere EPI/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 4-18.** 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 <a href="http://support.microsoft.com">http://support.microsoft.com</a>
MS PowerShell-Ausführungsrichtlinie	Die MS-PowerShell-Ausführungsrichtlinie muss auf <b>RemoteSigned</b> oder <b>Nicht eingeschränkt</b> 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

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- Stellen Sie sicher, dass Sie alle „[Anforderungen für Visual Basic-Skripterstellung](#)“, auf Seite 123 erfüllen.
- „[Herunterladen des Installationsprogramms für vRealize Automation IaaS](#)“, auf Seite 81.

### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.do-main.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

- 13 Konfigurieren Sie eine Verbindung zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 14 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.

#### Vorgehensweise

- 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

- Die IaaS-Komponenten, einschließlich Manager Service und Website, sind installiert.
- Stellen Sie sicher, dass Sie alle Anforderungen erfüllt haben. Informieren Sie sich unter [„Aktivieren von Remote-WMI-Anforderungen auf Windows-Maschinen“](#), auf Seite 125.
- [„Herunterladen des Installationsprogramms für vRealize Automation IaaS“](#), auf Seite 81.

### Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Setupdatei `setup__vra-va-hostname.domain.name@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 vRealize Automation-Appliance-Zertifikat im Client-Browser anzeigen, wenn auf die Verwaltungskonsole auf 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.
- 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
<b>Installation von redundanten Agents</b>	Installieren Sie redundante Agents auf unterschiedlichen Servern. Benennen und konfigurieren Sie redundante Agents identisch.
<b>Installation eines einzelnen Agents</b>	Wählen Sie einen eindeutigen Namen für diesen Agent aus.

- 13 Konfigurieren Sie eine Verbindung zur Manager Service-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager Service-Komponente ein. Beispielsweise <b>manager-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager Service-Komponente installiert haben. Beispielsweise <b>manager_service.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

Der Standardport lautet 443.

- 14 Konfigurieren Sie eine Verbindung zur Manager-Website-Komponente.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts für die Manager-Website-Komponente ein. Beispielsweise <b>website-load-balancer.eng.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Maschine ein, auf der Sie die Manager-Website-Komponente installiert haben. Beispielsweise <b>website_component.mycompany.com:443</b> . IP-Adressen werden nicht erkannt.

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.





# vRealize Automation -Aufgaben nach der Installation

# 5

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

Dieses Kapitel behandelt die folgenden Themen:

- „Ersetzen von selbstsignierten Zertifikaten mit von einer Zertifizierungsstelle bereitgestellten Zertifikaten“, auf Seite 129
- „Installieren des vRealize Log Insight-Agents auf IaaS-Servern“, auf Seite 129
- „Konfigurieren des Zugriffs auf den Standardmandanten“, auf Seite 129

## 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*.

## 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.

## 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.

## Vorgehensweise

- 1 Melden Sie sich bei der vRealize Automation-Konsole als Systemadministrator des Standardmandanten an.
  - a Navigieren Sie zur vRealize Automation-Konsole.

Option	Beschreibung
<b>Wenn Sie keinen Lastausgleichs-dienst verwenden</b>	<a href="https://vrealize-appliance-hostname.domain.name/vcac">https://vrealize-appliance-hostname.domain.name/vcac</a>

- 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**.

## Weiter

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. Ein Beispiel für das Anfordern des Elements und das Abschließen der manuellen Benutzeraktion finden Sie unter *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.



# Fehlerbehebung bei einer vRealize Automation -Installation

# 6

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

Dieses Kapitel behandelt die folgenden Themen:

- [„Standardspeicherorte für Protokolle“](#), auf Seite 133
- [„Rollback einer fehlgeschlagenen Installation wird ausgeführt“](#), auf Seite 134
- [„Erstellen eines vRealize Automation-Support-Pakets“](#), auf Seite 136
- [„Allgemeine Fehlerbehebung bei der Installation“](#), auf Seite 137
- [„Fehlerbehebung bei der vRealize Automation-Appliance“](#), auf Seite 140
- [„Fehlerbehebung bei IaaS-Komponenten“](#), auf Seite 143
- [„Fehlerbehebung bei Anmeldefehlern“](#), auf Seite 150

## Standardspeicherorte für Protokolle

Informationen zu fehlgeschlagenen Installationen finden Sie in den System- und Produktprotokolldateien.

Die angezeigten Dateipfade sind die Standardpfade. Wenn Sie IaaS in einem anderen Verzeichnis installiert haben, navigieren Sie stattdessen zu Ihrem benutzerdefinierten Installationsverzeichnis.

---

**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 erhalten Sie unter [VMware Solution Exchange](#).

---

## 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 Wapi-Configuration-<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 Softwarelebenszykluskripts	/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-IaaS-Installation vollständig installieren zu können.

### Vorgehensweise

- 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 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, vRealize Automation und WAPI entfernt wurden, und ob die Anwendungspools RepositoryAppPool, vCACAppPool und WapiAppPool ebenso entfernt wurden.

Die Installation wurde vollständig entfernt.

## Rollback einer verteilten Installation ausführen

Ein Systemadministrator muss einige Dateien manuell entfernen und die Datenbank zurücksetzen, um eine fehlgeschlagene IaaS-Installation vollständig installieren zu können.

### Vorgehensweise

- 1 Wenn die folgenden Komponenten vorhanden sind, deinstallieren Sie diese mit dem Windows-Deinstallationsprogramm.

- vRealize Automation-Server
- vRealize Automation-WAPI

---

**HINWEIS** Wenn die folgende Meldung angezeigt wird, starten Sie die Maschine neu und führen Sie diesen Vorgang aus: Fehler beim Öffnen der Installationsprotokolldatei. Stellen Sie sicher, dass der angegebene Speicherort vorhanden und nicht schreibgeschützt ist.

---



---

**HINWEIS** Wenn das Windows-System zurückgesetzt wurde oder Sie IaaS deinstalliert haben, müssen Sie den Befehl `iisreset` ausführen, bevor Sie vRealize Automation-IaaS erneut installieren.

---

- 2 Setzen Sie Ihre Datenbank auf den Zustand zurück, der vor der Installation bestand. Die verwendete Methode hängt vom Installationsmodus der ursprünglichen Datenbank ab.
- 3 Wählen Sie in IIS (Internet Information Services) die Standard-Website (oder Ihre benutzerdefinierte Site) aus und klicken Sie auf **Bindungen**. Entfernen Sie die https-Bindung (standardmäßig 443).
- 4 Prüfen Sie, ob das Anwendungs-Repository, vCAC und WAPI entfernt wurden, und ob die Anwendungspools RepositoryAppPool, vCACAppPool und WapiAppPool ebenso entfernt wurden.

**Tabelle 6-1.** 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.
Installieren von DEM Worker	Deinstallieren Sie alle DEM Workers, 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 vRealize Automation-Appliance-Verwaltungsschnittstelle erstellen. Support-Pakete erfassen Protokolle und helfen Ihnen oder dem technischen Support von VMware bei der Behebung von vRealize Automation-Problemen.

### Vorgehensweise

- 1 Öffnen Sie die vRealize Automation-Appliance-Verwaltungsschnittstelle in einem Webbrowser.  
<https://vrealize-automation-appliance-FQDN:5480>
- 2 Melden Sie sich als Root-Benutzer an und klicken Sie auf **vRA-Einstellungen > Cluster**.
- 3 Klicken Sie auf **Support-Paket erstellen**.
- 4 Klicken Sie auf **Herunterladen** und speichern Sie die Support-Paket-Datei auf Ihrem System.

Support-Pakete enthalten Informationen der vRealize Automation-Appliance- und IaaS-Windows-Server. Wenn die Verbindung zwischen den vRealize Automation-Appliance- und 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 vRealize Automation Management-Agent-Dienst auf IaaS-Windows-Servern, die in Rot angezeigt werden, angehalten wurde.

Informationen zu einem Sicherungsvorgang für das Erfassen von Protokollpaketen für IaaS-Komponenten finden Sie im [VMware Knowledgebase-Artikel 2078179](#).



## 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. Bearbeiten Sie beispielsweise, je nach verwendetem Lastausgleichsdienst, den Zeitüberschreitungswert für den Lastausgleichsdienst in Ihrer Konfigurationsdatei `ssl.conf` oder `httpd.conf` oder aber in einer anderen Web-Konfigurationsdatei.
- 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

Aktivieren Sie für jeden vRealize Automation-Appliance-Server und alle Windows-Server, auf denen IaaS-Komponenten installiert werden, die Zeitsynchronisierung so wie in den folgenden Themen beschrieben:

- „Aktivieren der Zeitsynchronisierung in der vRealize Automation Appliance“, auf Seite 54
- „Aktivieren der Zeitsynchronisierung auf dem Windows-Server“, auf Seite 59

Eine Übersicht über die Zeiterfassung bei vRealize Automation erhalten Sie unter „Uhrzeitsynchronisierung“, auf Seite 32.

## Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 werden möglicherweise leere Seiten angezeigt

Wenn Sie Internet Explorer 9 oder 10 unter Windows 7 verwenden und der Kompatibilitätsmodus aktiviert ist, scheinen manche Seiten keinen Inhalt aufzuweisen.

### Problem

Bei Verwendung von Internet Explorer 9 oder 10 unter Windows 7 weisen die folgenden Seiten keinen Inhalt auf:

- Infrastruktur
- Standardmandantenordner auf der Orchestrator-Seite
- Serverkonfiguration auf der Orchestrator-Seite

### Ursache

Dieses Problem könnte darauf zurückzuführen sein, dass der Kompatibilitätsmodus aktiviert ist. Den Kompatibilitätsmodus können Sie für Internet Explorer wie folgt deaktivieren.

### Lösung

#### Voraussetzungen

Stellen Sie sicher, dass die Menüleiste angezeigt wird. Wenn Sie Internet Explorer 9 oder 10 verwenden, drücken Sie die Alt-Taste, um die Menüleiste anzuzeigen (oder klicken Sie mit der rechten Maustaste auf die Adressleiste und wählen Sie **Menüleiste** aus).

#### Vorgehensweise

- 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 Zertifikatsfehler 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 die Datei `vcac-config.exe.config` und suchen Sie nach der Repository-Adresse: `<add key="repositoryAddress" value="https://[IaaS address]:443/repository/" />`
- 2 Navigieren Sie in Internet Explorer zu dieser Adresse.
- 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 dieses Zertifikat nicht vertrauenswürdig ist.

Falls die Probleme weiterhin bestehen, wiederholen Sie den Vorgang mit der Adresse, die registriert werden muss, nämlich der Endpoint-Adresse, die Sie zum Registrieren mit „vcac-config.exe“ verwendet haben.

## Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server

Bestimmte Sites stellen unter Umständen über einen Proxy-Server eine Verbindung zum Internet her.

### Problem

Ihre Bereitstellung kann keine Verbindung zum offenen Internet herstellen. Sie können beispielsweise nicht auf Websites, öffentliche Clouds, die von Ihnen verwaltet werden, oder Anbieteradressen zugreifen, die Sie zum Herunterladen von Software oder Updates benötigen.

### Ursache

Ihre Site stellt über einen Proxy-Server eine Verbindung zum Internet her.

### Lösung

#### Voraussetzungen

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

#### Vorgehensweise

- 1 Verweisen Sie mit einem Webbrowser auf die Verwaltungskonsolle der vRealize Automation-Appliance:  
`https://appliance-FQDN-or-IP-address:5480`
- 2 Melden Sie sich mit dem beim Bereitstellen der Appliance festgelegten Benutzernamen **root** und Kennwort an.
- 3 Klicken Sie auf die Registerkarte **Netzwerk**.
- 4 Geben Sie den FQDN oder die IP-Adresse und Portnummer des Proxy-Servers Ihrer Site ein.
- 5 Benötigt der Proxy-Server Anmeldedaten, geben Sie den Benutzernamen und das Kennwort ein.
- 6 Klicken Sie auf **Einstellungen speichern**.

### Weiter

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 Anmeldung von VMware Identity Manager-Benutzern“](#), auf Seite 151.

## Konsolenschritte für die Erstkonfiguration von Inhalten

Es steht eine Alternative zur Verwendung der vRealize Automation-Installationsschnittstelle zum Erstellen des Kontos für den Konfigurationsadministrator und des anfänglichen Inhalts zur Verfügung.

### Problem

Im letzten Teil der Installation von vRealize Automation führen Sie das Verfahren zum Erstellen eines neuen Kontos, des lokalen Benutzerkontos „configurationadmin“ und des anfänglichen Inhalts durch. Ein Fehler tritt auf und die Schnittstelle wird in einen nicht behebbaren Zustand versetzt.

## Lösung

Statt die Schnittstelle zu verwenden, geben Sie Konsolenbefehle ein, um den Benutzer „configurationadmin“ und den anfänglichen Inhalt zu erstellen. Beachten Sie, dass die Schnittstelle möglicherweise erst nach der erfolgreichen Durchführung eines Teils des Verfahrens ausfällt, sodass Sie ggf. nur einige der Befehle benötigen.

Angenommen, Sie untersuchen die Protokolle und die Ausführung des vRealize Orchestrator-Workflows und stellen dabei fest, dass der Benutzer „configurationadmin“ durch das schnittstellenbasierte Setup erstellt wurde, der anfängliche Inhalt aber nicht. In diesem Fall können Sie einfach die letzten beiden Konsolenbefehle eingeben, um das Verfahren abzuschließen.

### Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Appliance-Konsole 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
```

## 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 aus der vRealize Automation-Appliance heruntergeladen werden.

#### Problem

Installationsprogramme werden beim Ausführen von `setup__vra-va-hostname.domain.name.exe` nicht heruntergeladen.

#### Ursache

- Probleme mit der Netzwerkkonnektivität beim Herstellen der Verbindung zur vRealize Automation-Appliance-Maschine.

- Herstellung der Verbindung zur vRealize Automation-Appliance-Maschine 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-Appliance-Maschine herstellen können, indem Sie die folgende URL in einen Webbrowser eingeben.  
`https://vra-va-hostname.domain.name`
- 2 Lesen Sie die anderen Abschnitte zur Fehlerbehebung bei der vRealize Automation-Appliance.
- 3 Laden Sie die Setupdatei herunter und stellen Sie die Verbindung zur vRealize Automation-Appliance erneut her.

## Falsche Berechtigungen für die Datei „Encryption.key“

Ein Systemfehler kann verursacht werden, wenn der Datei „Encryption.key“ für eine virtuelle Appliance falsche Berechtigungen zugewiesen werden.

### Problem

Sie melden sich bei der vRealize Automation-Appliance an und die Seite „Mandanten“ wird angezeigt. Nachdem das Laden der Seite gestartet wurde, wird die Meldung Systemfehler angezeigt.

### Ursache

Die Datei „Encryption.key“ weist falsche Berechtigungen auf oder die Gruppen- oder Besitzerbenutzerebene ist nicht ordnungsgemäß zugewiesen.

### Lösung

#### Voraussetzungen

Melden Sie sich bei der virtuellen Appliance an, in der die Fehlermeldung angezeigt wird.

---

**HINWEIS** Wenn Ihre virtuellen Appliances unter einem Lastausgleichsdienst ausgeführt werden, müssen Sie jede virtuelle Appliance überprüfen.

---

#### Vorgehensweise

- 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.

### Weiter

Melden Sie sich bei der Seite „Mandanten“ an, um sicherzustellen, dass Sie sich problemlos anmelden können.

## Identity Manager startet nach einem Neustart von horizon-workspace nicht

In einer vRealize Automation-Umgebung mit Hochverfügbarkeit kann es vorkommen, dass der Identity Manager nach einem Neustart des horizon-workspace-Dienstes nicht startet.

### Problem

Der horizon-workspace-Dienst kann aufgrund eines Fehlers wie dem Folgenden nicht starten:

Fehler beim Erstellen von Bean mit dem Namen 'liquibase', definiert in der Klassenpfadresource [spring/datastore-wireup.xml]: Aufruf der init-Methode fehlgeschlagen; verschachtelte Ausnahme ist liquibase.exception.LockException: Änderungsprotokollsperrung konnte nicht angefordert werden. Derzeit gesperrt durch fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) seit 10/29/15

### Ursache

Der Identity Manager startet möglicherweise in einer Hochverfügbarkeitsumgebung aufgrund von Problemen mit dem liquibase-Datenverwaltungsdienstprogramm nicht, das von vRealize Automation verwendet wird.

### Lösung

- 1 Melden Sie sich bei der vRealize Automation-Appliance als Root-Benutzer mithilfe von SSH an.
- 2 Führen Sie den Befehl `service horizon-workspace` aus, um den horizon-workspace-Dienst anzuhalten.
- 3 Führen Sie den Befehl `su postgres` aus, um Postgres-Benutzer zu werden.
- 4 Führen Sie den Befehl `psql vcac` aus:
- 5 Führen Sie die folgende SQL-Anweisung aus: `"update "databasechangelock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`
- 6 Führen Sie die SQL-Abfrage `select *` über `databasechangelock` aus.  
Die Ausgabe sollte einen Wert von „f“ für gesperrt anzeigen.
- 7 Starten Sie den horizon-workspace-Dienst mit dem Befehl `service horizon-workspace start`.

## Falsche Zuweisungen von Appliance-Rollen nach Failover

Nachdem ein Failover stattgefunden hat, haben die Master- und Replikatknoten der vRealize Automation-Appliance möglicherweise nicht die richtige Rollenzuweisung. Davon sind alle Dienste betroffen, die Schreibzugriff für die Datenbank benötigen.

### Problem

In einem Hochverfügbarkeitscluster mit vRealize Automation-Appliances fahren Sie den Master-Datenbankknoten herunter oder sorgen dafür, dass kein Zugriff darauf mehr möglich ist. Über die Verwaltungskonsole auf einem anderen Knoten stufen Sie diesen Knoten zum neuen Master-Knoten herauf. Dadurch wird der Schreibzugriff auf die vRealize Automation-Datenbank wiederhergestellt.

Zu einem späteren Zeitpunkt stellen Sie den alten Master-Knoten wieder online. Auf der Registerkarte „Datenbank“ in der Verwaltungskonsole dieses Knotens wird dieser weiterhin als Master-Knoten aufgeführt, obwohl er es nicht ist. Versuche, das Problem über die Verwaltungskonsole eines anderen Knotens zu lösen, indem der alte Knoten offiziell wieder zum Master-Knoten heraufgestuft wird, schlagen fehl.

### Lösung

Befolgen Sie bei einem Failover diese Richtlinien beim Konfigurieren von alten im Vergleich zu neuen Master-Knoten.

- Bevor Sie einen anderen Knoten zum Master-Knoten heraufstufen, entfernen Sie den vorherigen Master-Knoten aus dem Lastenausgleichspool von vRealize Automation-Appliance-Knoten.

- Damit vRealize Automation einen alten Master-Knoten wieder in den Cluster übernimmt, muss die alte Maschine online geschaltet werden. Öffnen Sie anschließend die Verwaltungskonsole des neuen Master-Knotens. Suchen Sie nach dem alten Knoten, der auf der Registerkarte „Datenbank“ als invalid aufgeführt ist, und klicken Sie auf die Schaltfläche **Zurücksetzen**.

Nach dem erfolgreichen Zurücksetzen können Sie den alten Knoten im Lastenausgleichspool der vRealize Automation-Appliance-Knoten wiederherstellen.

- Um einen alten Master-Knoten manuell wieder in den Cluster zu übernehmen, schalten Sie die Maschine online und fügen Sie sie dem Cluster so hinzu, als handelte es sich um einen neuen Knoten. Geben Sie beim Hinzufügen den neu heraufgestuften Knoten als primären Knoten an.

Nachdem der Knoten erfolgreich hinzugefügt wurde, können Sie den alten Knoten im Lastenausgleichspool der vRealize Automation-Appliance-Knoten wiederherstellen.

- Verwenden Sie die Verwaltungskonsole eines alten Master-Knotens erst wieder für Clusterverwaltungsvorgänge, nachdem der alte Master-Knoten ordnungsgemäß zurückgesetzt oder dem Cluster wieder hinzugefügt wurde, auch wenn der Knoten wieder online geschaltet wurde.
- Nachdem Sie den Knoten ordnungsgemäß zurückgesetzt oder wieder hinzugefügt haben, können Sie einen alten Knoten wieder zum Master-Knoten heraufstufen.

## 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.

### 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:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Geben Sie einen Befehls im Format `Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v` ein. Optionale Parameter sind `-su [SQL user name]` und `-sp [password]`.

Ist der Befehl erfolgreich, wird die folgende Meldung angezeigt:

```
Certificates validated successfully.
Command succeeded."
```

Schlägt der Befehl fehl, wird eine detaillierte Fehlermeldung angezeigt.

---

**HINWEIS** Dieser Befehl ist nur auf dem Knoten für die Model Manager-Datenkomponente verfügbar.

---

## Fehler aufgrund der Anmeldedaten beim Ausführen des IaaS-Installers

Wenn Sie IaaS-Komponenten installieren, erhalten Sie eine Fehlermeldung bei der Eingabe der Anmeldedaten für die virtuelle Appliance.

### Problem

Nach der Eingabe der Anmeldedaten in den IaaS-Installer wird ein `org.xml.sax.SAXParseException`-Fehler angezeigt.

### Ursache

Sie haben falsche Anmeldedaten oder ein falsches Format für die Anmeldedaten verwendet.

### Lösung

- ◆ Stellen Sie sicher, dass Sie die richtigen Mandanten- und Benutzernamenwerte verwenden.

Der SSO-Standardmandant verwendet beispielsweise einen 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 von 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 von vRealize Automation-Appliance aufgrund ungültiger `msiexec`-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-Daten und Webkomponenten 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 der 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

Überprüfen Sie, ob Sie eine Verbindung zur vRealize Automation-Appliance-Maschine herstellen können, indem Sie die folgende URL in einen Webbrowser eingeben: `https://vra-va-hostname.domain.name`.

### ■ 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.
- Prüfen Sie über einen Browser `https://<ip-web>/repository/data/MetaModel.svc` und stellen Sie sicher, dass in Ihrem Browser kein Zertifikatsfehler angezeigt wird.

### ■ 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 Zertifikathierarchie verwenden.

### ■ Repository-Dienst

Führen Sie folgende Aktionen durch, um den Status des Repository-Diensts zu überprüfen.

- Überprüfen Sie über einen Browser den Status des Metamodell-Diensts unter `https://<ip-web>/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 *c0DD0C01*.
- 3 Suchen Sie in der Protokolldatei nach dem Referenzcode, um den zugehörigen Eintrag aufzufinden.
- 4 Überprüfen Sie die Einträge, die über und unter dem zugehörigen Eintrag angezeigt werden, um eine Fehlerbehebung des Problems vorzunehmen.

Der zugehörige Protokolleintrag verweist nicht spezifisch auf die Ursache des Problems.

**Ein Proxy-Agent kann nicht deinstalliert werden**

Das Entfernen eines Proxy-Agents kann fehlschlagen, wenn die Windows Installer-Protokollierung aktiviert ist.

**Problem**

Wenn Sie versuchen, einen Proxy-Agent von der Windows-Systemsteuerung zu deinstallieren, schlägt die Deinstallation fehl und die folgende Fehlermeldung wird angezeigt:

Error opening installation log file. Verify that the specified log file location exists and is writable

**Ursache**

Dies kann auftreten, wenn die Windows Installer-Protokollierung aktiviert ist, aber die Windows Installer-Engine kann die Deinstallations-Protokolldatei nicht ordnungsgemäß schreiben. Weitere Informationen finden Sie im [Microsoft Knowledgebase-Artikel 2564571](#).

## Lösung

- 1 Starten Sie die Maschine neu oder starten Sie explorer.exe über den Task-Manager neu.
- 2 Deinstallieren Sie den Agent.

## Fehler bei Maschinenanforderungen, wenn Remote-Transaktionen deaktiviert sind

Es kommt zu einem Fehler bei Maschinenanforderungen, wenn DTC-Remote-Transaktionen (Microsoft Distributed Transaction Coordinator) auf Windows-Server-Maschinen deaktiviert sind.

### Problem

Wenn Sie eine Maschine bereitstellen, wenn Remote-Transaktionen auf dem Model Manager-Portal oder dem SQL Server deaktiviert sind, wird die Anforderung nicht abgeschlossen. Es kommt zu einem Fehler bei der Datenerfassung, und die Maschinenanforderung verbleibt in einem Status für den Klonworkflow.

### Ursache

DTC-Remote-Transaktionen sind in der IaaS-SQL-Instanz deaktiviert, die von dem vRealize Automation-System verwendet wird.

### Lösung

- 1 Starten Sie Windows Server Manager zum Aktivieren von DTC auf allen vRealize-Servern und zugeordneten SQL-Servern.

Navigieren Sie in Windows 7 zu **Start > Verwaltungstools > Komponentendienste**.

---

**HINWEIS** Stellen Sie sicher, dass alle Windows-Server über eindeutige SIDs für die MSDTC-Konfiguration verfügen.

---

- 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 vRealize Automation-Appliance an.  
`https://virtualappliancename/vcac/tenantname`
  - 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-Knoten, die über eine Vorlage geklont werden, in der MS DTC installiert ist, enthalten doppelte Bezeichner für MS 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 angezeigt.

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-Knoten klonen, in dem MS DTC installiert ist, verwenden beide Klone denselben eindeutigen Bezeichner für MS DTC. Die Kommunikation zwischen den Knoten schlägt fehl.

### Lösung

- 1 Öffnen Sie als Administrator eine Eingabeaufforderung.
- 2 Führen Sie den folgenden Befehl aus: `msdtc -uninstall`
- 3 Starten Sie die virtuelle Maschine neu.
- 4 Öffnen Sie eine separate Eingabeaufforderung und führen Sie den folgenden Befehl aus:  
`msdtc -install <manager-service-host>.`

## Geändertes Verhalten für die Anpassung von E-Mails

In vRealize Automation 6.0 oder höher können nur die von der IaaS-Komponente generierten Benachrichtigungen mithilfe der E-Mail-Vorlagenfunktion aus früheren Versionen angepasst werden.

### Lösung

Sie können die folgenden XSLT-Vorlagen verwenden:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified

- VdiRegister
- VdiUnregister

E-Mail-Vorlagen sind im Verzeichnis \Templates des Serverinstallationsverzeichnis gespeichert, in der Regel %SystemDrive%\Programme (x86)\VMware\VCAC\Server. Das Verzeichnis \Templates enthält auch XSLT-Vorlagen, die nicht mehr unterstützt werden und nicht geändert werden können.

## Fehlerbehebung bei Anmeldefehlern

Die Themen zur Fehlerbehebung bei Anmeldefehlern für vRealize Automation liefern Lösungen für potenzielle Probleme im Zusammenhang mit der Installation, die bei der Verwendung von vRealize Automation auftreten können.

### Anmeldeversuche als IaaS-Administrator mit falsch formatierten UPN-Anmeldedaten schlagen ohne Begründung fehl

Sie versuchen, sich bei vRealize Automation als IaaS-Administrator anzumelden und werden ohne Begründung an die Anmeldeseite weitergeleitet.

#### Problem

Wenn Sie versuchen, sich bei vRealize Automation als IaaS-Administrator mit UPN-Anmeldedaten ohne die Komponente „@<em>IhreDomäne</em>“ des Benutzernamens anzumelden, werden Sie von SSO sofort abgemeldet und ohne Begründung an die Anmeldeseite umgeleitet. </li>

#### 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 müssen. Andernfalls können Sie sich nicht anmelden.

#### Problem

Sie konfigurieren vRealize Automation für Hochverfügbarkeit durch Installation einer zusätzlichen vRealize Automation-Appliance. Wenn Sie versuchen, sich bei vRealize Automation anzumelden, wird eine Meldung über eine ungültige Lizenz angezeigt. Die Meldung ist jedoch falsch, da Sie ermittelt haben, dass Ihre Lizenz gültig ist.

#### Ursache

Die vRealize Automation-Appliance-Knoten bilden erst dann korrekt einen Hochverfügbarkeitscluster, wenn sie die kurzen Hostnamen der Knoten im Cluster auflösen können.

#### Lösung

Damit ein Cluster mit hochverfügbaren vRealize Automation-Appliances kurze Hostnamen auflösen kann, führen Sie eines der folgenden Verfahren durch. Sie müssen alle Appliances im Cluster ändern.

**Vorgehensweise**

- Bearbeiten oder erstellen Sie eine Suchzeile in der Datei `/etc/resolv.conf`. Die Zeile sollte Domänen mit vRealize Automation-Appliances enthalten. Trennen Sie mehrere Domänen durch Leerzeichen voneinander. Beispiel:

```
search eng.mycompany.com tech.mycompany.com
```

- Bearbeiten oder erstellen Sie Domänenzeilen in der Datei `/etc/resolv.conf`. Jede Zeile sollte Domänen mit vRealize Automation-Appliances enthalten. Beispiel:

```
domain eng.mycompany.com
```

- Fügen Sie der Datei `/etc/hosts` Zeilen hinzu, sodass jeder Kurzname einer vRealize Automation-Appliance ihrem vollqualifizierten Domännennamen zugeordnet wird. Beispiel:

```
node1    node1.eng.mycompany.com
node2    node2.eng.mycompany.com
```

**Proxy verhindert Anmeldung von VMware Identity Manager-Benutzern**

Wenn Sie die Verwendung eines Proxyserver konfigurieren, wird möglicherweise die Anmeldung von VMware Identity Manager-Benutzern verhindert.

**Problem**

Sie konfigurieren für vRealize Automation den Zugriff auf das Netzwerk über einen Proxyserver, und VMware Identity Manager-Benutzern wird beim Anmelden folgende Fehlermeldung angezeigt.

```
Error Unable to get metadata
```

**Lösung****Voraussetzungen**

Konfigurieren Sie vRealize Automation für den Zugriff auf das Netzwerk über einen Proxyserver. Siehe [„Herstellen einer Verbindung zum Netzwerk über einen Proxy-Server“](#), auf Seite 139.

**Vorgehensweise**

- 1 Melden Sie sich an 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=vra-hostname
```

```
Beispiel: NO_PROXY="localhost, 127.0.0.1, vra.system.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
```





# Hintergrundinstallation von vRealize Automation

# 7

vRealize Automation umfasst eine Option für eine Skriptinstallation im Hintergrund.

Bei der Hintergrundinstallation wird eine auf eine textbasierte Antwortdatei verweisende ausführbare Datei verwendet, in der Sie die System-FQDNs, Kontoanmeldedaten und andere Einstellungen vorab konfigurieren, die Sie normalerweise im Verlauf einer herkömmlichen assistentenbasierten oder manuellen Installation hinzufügen. Die Hintergrundinstallation ist bei folgenden Bereitstellungstypen nützlich:

- Bereitstellung mehrerer, nahezu identischer Umgebungen
- Wiederholte Bereitstellung derselben Umgebung
- Durchführen automatischer Installationen
- Durchführen von Skriptinstallationen

Dieses Kapitel behandelt die folgenden Themen:

- [„Ausführen einer unbeaufsichtigten vRealize Automation-Installation“](#), auf Seite 153
- [„Ausführen einer unbeaufsichtigten Installation des vRealize Automation-Management-Agents“](#), auf Seite 154
- [„Antwortdatei der unbeaufsichtigten vRealize Automation-Installation“](#), auf Seite 155
- [„Die vRealize Automation-Installationsbefehlszeile“](#), auf Seite 156

## Ausführen einer unbeaufsichtigten vRealize Automation -Installation

Sie können eine automatische, unbeaufsichtigte vRealize Automation-Installation über die Konsole einer neu bereitgestellten vRealize Automation-Appliance ausführen.

### Voraussetzungen

- Stellen Sie eine vRealize Automation-Appliance bereit, melden Sie sich jedoch nicht bei ihr an und starten Sie nicht den Installationsassistenten.
- 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 unbeaufsichtigten Installation des vRealize Automation-Management-Agents“](#), auf Seite 154 beschriebenen unbeaufsichtigten Vorgangs installieren.

### Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Appliance-Konsole 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 unbeaufsichtigte Installation speichert keine proprietären Daten im Protokoll (wie beispielsweise Kennwörter, Lizenzen oder Zertifikate).

## Ausführen einer unbeaufsichtigten Installation des vRealize Automation -Management-Agents

Sie können eine befehlszeilenbasierte Installation des vRealize Automation-Management-Agents auf jedem IaaS-Windows-Server ausführen.

Die unbeaufsichtigte 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 unbeaufsichtigte Installation des Management-Agents auf allen IaaS-Windows-Servern durchführen, indem Sie auf jedem einzelnen Kopien desselben Skripts ausführen.

### Voraussetzungen

- Stellen Sie die vRealize Automation-Appliance bereit.
- Erstellen oder identifizieren Sie die IaaS-Windows-Server und konfigurieren Sie dazugehörige Voraussetzungen.

### Vorgehensweise

- 1 Verweisen Sie auf dem IaaS-Windows-Server einen Webbrowser auf die folgende URL auf der vRealize Automation-Appliance.

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

- 2 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.

- 3 Öffnen Sie die Datei `InstallManagementAgent.ps1` in einem Texteditor.

- 4 Fügen Sie im oberen Bereich der Skriptdatei die bereitstellungsspezifischen Einstellungen hinzu.

- Die URL der vRealize Automation-Appliance

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

- Anmeldedaten für das vRealize Automation-Appliance-Root-Benutzerkonto

- 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
- 5 Speichern und schließen Sie `InstallManagementAgent.ps1`.
  - 6 Doppelklicken Sie für eine unbeaufsichtigte Installation des Management-Agents auf `InstallManagementAgent.ps1`.
  - 7 (Optional) Stellen Sie sicher, dass die Installation abgeschlossen ist, indem Sie **VMware vCloud Automation Center-Management-Agent** in der Liste der Programme und Funktionen in der Windows-Systemsteuerung sowie in der Liste der ausgeführten Windows-Dienste suchen.

## Antwortdatei der unbeaufsichtigten vRealize Automation -Installation

Für die unbeaufsichtigte vRealize Automation-Installation ist die Vorbereitung einer textbasierten Antwortdatei im Vorfeld erforderlich.

Eine neu bereitgestellte vRealize Automation-Appliance enthält eine Standardantwortdatei.

`/usr/lib/vcac/tools/install/ha.properties`

Um eine unbeaufsichtigte Installation auszuführen, müssen Sie unter Verwendung eines Texteditors die Einstellungen in `ha.properties` an die zu installierende Bereitstellung anpassen. Die folgenden Beispiele sind nur einige der Einstellungen und Informationen, die Sie hinzufügen müssen.

- Der vRealize Automation- oder Suite-Lizenzschlüssel
- FQDNs der vRealize Automation-Appliance-Knoten
- Anmeldedaten für das vRealize Automation-Appliance-Root-Benutzerkonto
- IaaS-Windows-Server-FQDNs, die als Web-Knoten, Manager Service-Knoten usw. agieren
- Anmeldedaten für den vRealize Automation-Dienstbenutzer, ein Domänenkonto mit Administratorberechtigungen auf den IaaS-Windows-Servern
- FQDNs der Lastausgleichsdienste
- Parameter der SQL Server-Datenbank
- Proxy-Agent-Parameter für die Herstellung der Verbindung zu Virtualisierungsressourcen
- Die Information, ob das Programm für die unbeaufsichtigte Installation versuchen sollte, fehlende Voraussetzungen für IaaS-Windows-Server zu korrigieren

Das Programm für die unbeaufsichtigte Installation kann viele fehlende Windows-Voraussetzungen korrigieren. Einige Konfigurationsprobleme wie beispielsweise unzureichende CPU können jedoch nicht durch das Programm für die unbeaufsichtigte Installation geändert werden.

Um Zeit einzusparen, können Sie die Datei `ha.properties` wiederverwenden und ändern, die für eine andere Bereitstellung konfiguriert wurde. Es muss sich dabei um eine Bereitstellung handeln, bei der die Einstellungen ähnlich waren. Wenn Sie vRealize Automation über den Installationsassistenten installieren, erstellt der Assistent die Einstellungen in der Datei `ha.properties` und speichert sie in dieser Datei. Die Datei kann für die Wiederverwendung und Änderung bei der Durchführung einer unbeaufsichtigten Installation einer ähnlichen Bereitstellung hilfreich sein.

Der Assistent speichert keine proprietären Einstellungen in der Datei `ha.properties` (wie beispielsweise Kennwörter, Lizenzen oder Zertifikate).

## Die vRealize Automation -Installationsbefehlszeile

vRealize Automation enthält eine konsolenbasierte Befehlszeilenschnittstelle für die Durchführung von Installationsanpassungen, die nach der Erstinstallation erforderlich sein können.

Die Befehlszeilenschnittstelle (Command Line Interface, CLI) kann Installations- und Konfigurationsaufgaben ausführen, die nach der Erstinstallation über die browserbasierte Schnittstelle nicht mehr verfügbar sind. Zu den CLI-Funktionen zählen die erneute Überprüfung der Voraussetzungen, die Installation von IaaS-Komponenten, die Installation von Zertifikaten oder die Festlegung des vRealize Automation-Hostnamens, auf den Benutzer in ihren Webbrowsern verweisen.

Die CLI ist außerdem nützlich für erfahrene Benutzer, die für bestimmte Vorgänge Skripts erstellen möchten. Einige CLI-Funktionen werden bei der automatischen Installation verwendet. Wenn Sie mit beiden Funktionen vertraut sind, können Sie Ihre Kenntnisse der Installationsskripts für vRealize Automation vertiefen.

### Installation von vRealize Automation über die Befehlszeile – Grundlagen

Die Befehlszeilenschnittstelle für die vRealize Automation-Installation verfügt über drei Grundfunktionen.

Die Grundfunktionen sind das Anzeigen der vRealize Automation-Knoten-IDs, das Ausführen von Befehlen und das Anzeigen der Hilfeinformationen. Geben Sie den folgenden Befehl ohne Optionen oder Bezeichner ein, um diese Vorgänge in der Konsolenansicht anzuzeigen.

```
vra-command
```

#### Anzeigen von Knoten-IDs

Sie müssen die vRealize Automation-Knoten-IDs kennen, um Befehle für die richtigen Zielsysteme ausführen zu können. Geben Sie zum Anzeigen der Knoten-IDs den folgenden Befehl ein.

```
vra-command list-nodes
```

Notieren Sie sich die Knoten-IDs, bevor Sie die Befehle ausführen.

#### Ausführen von Befehlen

Die meisten Befehlszeilenfunktionen umfassen das Ausführen eines Befehls für einen Knoten im vRealize Automation-Cluster. Verwenden Sie die folgende Syntax, um einen Befehl auszuführen.

```
vra-command execute --node Knoten-ID Befehlsname --Parametername Parameterwert
```

Wie in der vorherigen Syntax gezeigt, erfordern viele Befehle vom Benutzer ausgewählte Parameter und Parameterwerte.

#### Anzeigen 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-IaaS-Datenbank
- Ausführen der Voraussetzungsprüfung für einen IaaS-Windows-Server
- Importieren von Zertifikaten

Um eine vollständige Liste der verfügbaren vRealize Automation-Befehle anzuzeigen, melden Sie sich bei der vRealize Automation-Appliance-Konsole 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
```



# Index

## A

### Agenten

Auswählen des Installationsszenarios **106**

Hyper-V **112**

Installieren **104**

Installieren der vSphere-Agents **108**

konfigurieren, vSphere-Agents **111**

XenServer **112**

### Agents

Aktivieren von Remote-WMI-Anforderungen **125**

EPI PowerShell **17**

Hyper-V **112**

Installationsspeicherort und Anforderungen **106**

Installieren der Citrix-Agents **120**

Installieren des EPI-Agents für Citrix **119**

Installieren des EPI-Agents für Visual Basic-Skripterstellung **122**

Installieren für Visual Basic-Skripterstellung **123**

Installieren von WMI **126**

installieren von XenDesktop **117**

Integrations-Agents **17**

Konfigurieren von Hyper-V **115**

Konfigurieren von XenServer **115**

VDI PowerShell **17**

Visual Basic-Anforderungen bei Skripterstellung **123**

WMI-Agents **17**

XenServer **112**

### Aktualisierte Informationen **9**

### Anforderungen

Datenbank **21**

DEM **23**

SQL **21**

### Anmeldefehler

Fehlerbehebung **150**

Server sind nicht synchron **137**

Anmeldung als IaaS-Administrator schlägt fehl **150**

Antwortdatei, Hintergrundinstallation **155**

Anwendungsfälle, Hintergrundinstallation **153**

Appliances, Konfigurieren zusätzlicher **77**

Aufgaben nach der Installation, Konfigurieren des Windows-Diensts für den Zugriff auf die IaaS-Datenbank **102**

Authentifizierung **103**

## B

Befehlszeile **156, 157**

Bereitstellungsparameter, festlegen **40, 48**

Bereitstellungspfad

Auswählen **11**

Verteilte Installation **11**

Bereitstellungsserver **119**

Bereitstellungsszenario

Minimalbereitstellung **51**

Minimalinstallation **11**

Verteilte Bereitstellung **64**

## C

Citrix, Installieren des EPI-Agents **119**

Citrix-Agents, Installieren **120**

Cluster;Hinzufügen **78**

## D

### Datenbank

Anforderungen **21**

Erstellen mithilfe des Assistenten **85**

Vorbereiten der IaaS-Datenbank **82**

Deinstallieren, fehlgeschlagene Installation **135**

### DEM

Anforderungen **23**

Info zur Installation **99**

Installieren **100**

OpenStack-Anforderungen **25**

PowerVC-Anforderungen **25**

DEM-Worker, Verbindungsherstellung mit SCVMM **102**

### DEMs

Anforderungen für Amazon Web Services EC2 **24**

Anforderungen für Red Hat **25**

Installation schlägt fehl **144**

SCVMM-Anforderungen **25**

Distributed Execution Manager

*Siehe auch* DEM

*Siehe auch* DEM

Distributed Transaction Coordinator (DTC) **21**

DTC (Distributed Transaction Coordinator) **21**

## E

- E-Mail-Anpassungen **149**
- Encryption.key (Datei), Festlegen von Berechtigungen **141**
- Endpoints
  - DEM-Anforderungen für OpenStack **25**
  - DEM-Anforderungen für PowerVC **25**
- EPI-Agents, Installieren für Visual Basic-Skripterstellung **122, 123**
- Erstellung von anfänglichem Inhalt, Fehlerbehebung **139**
- Erstkonfiguration von Inhalten, Kennwort erstellen **42, 50**

## F

- Federal Information Processing Standard (FIPS) **146**
- Fehler bei Maschinenanforderung **148**
- Fehlerbehebung
  - Anzeige leerer Seiten **138**
  - geklonte IaaS-Knoten **149**
  - IaaS-Installationsprogramm **144**
  - Maschinenanforderungen **148**
  - Master-Knoten fehlerhaft **142**
  - Protokollspeicherorte **133**
  - Serverzeiten sind nicht synchron **137**
- Fehlerbehebung bei der Installation **137**
- Fehlerbehebung, Installation **133**
- Fehlgeschlagene Installation, Protokolle **133**
- FIPS (Federal Information Processing Standard) **146**

## G

- Geklonte IaaS-Knoten **149**

## H

- Hintergrundinstallation
  - Antwortdatei **155**
  - Anwendungsfälle **153**
  - Management-Agent **154**
  - vRealize Automation **153**
- Hyper-V
  - Agent **112**
  - Anforderungen **112**
  - Proxy-Agent **112**
- Hyper-V-Agents, Installieren **112**
- Hypervisor, Anforderungen **112**

## I

- IaaS
  - Agents **17**
  - herunterladen, Installationsprogramm **81**
- IaaS Manager Service, Anforderungen **23**
- IaaS-Administratoren, erstellen **129**
- IaaS-Authentifizierung, Ausfall **145**

## IaaS-Datenbank

- Erstellen der Datenbank **84**
- Erstellen der Datenbank mithilfe des Assistenten **85**
- Konfigurieren des Windows-Diensts für den Zugriff **102**
- Konfigurieren für sicheres SSL **62, 82–85**
- Manuelles Erstellen der Datenbank **83**
- SQL-Datenbank festlegen **62**
- IaaS-Datenbank, Zugriff auf, aktivieren über Dienstbenutzer **103**
- IaaS-Dienste, überprüfen **104**
- IaaS-Installationsprogramm
  - Fehlerbehebung **144**
  - herunterladen **60**
- IaaS-Komponenten
  - Fehlerbehebung **143**
  - Installieren **58**
  - installieren, in einer verteilten Konfiguration **79**
  - registrieren **63**
- IaaS-Komponenten, Definition **65**
- Identitätsquelle, Domänen-Anforderungen **29**
- Identity Manager, startet nicht **142**
- Infrastrukturkomponenten, Installieren **59**
- Installation
  - Abschließen **41, 49, 64**
  - Agenten angeben **63**
  - DNS- und Hostnamensauflösung **19**
  - Fehlerbehebung **133**
  - Manager angeben **63**
  - nach der Installation **129**
  - Überblick über die Minimalinstallation **52**
  - Überblick über Minimalbereitstellung **13**
  - Übersicht **11**
  - Übersicht über die verteilte Bereitstellung **13**
  - Verwenden der Verwaltungskonsole **51**
  - Vorbereitung **19**
  - vRealize Automation-Appliance **52, 72**
- Installation Download, Fehlerbehebung **140**
- Installationsanforderungen
  - Anmeldedaten **29**
  - Benutzer **29**
  - Bereitstellungsumgebungen **20**
  - Betriebssystem **20**
  - Hardware **20**
  - IaaS-Anforderungen **22**
  - Portanforderungen **26**
  - Sicherheit **30**
  - Virtuelle Maschine **20**
  - Windows Server **21**
  - XenDesktop **116**



Installationsassistent  
 Übersicht **33**  
 Unternehmensbereitstellung **43**  
 Installationsfehler, Server sind nicht syn-  
 chron **137**  
 Installationskomponenten  
 Auswählen eines Bereitstellungspaths **11**  
 Prüfen der Voraussetzungen **61**  
 SSO **15**  
 VMware Infrastructure-as-a-Service (IaaS) **15**  
 VMware vRealize Automation-Appliance **15**  
 Installationsparameter, Validierung **41, 49**  
 Installationstyp  
 Anmeldung **60**  
 auswählen **60**  
 Installationsvorbereitung, Uhrzeitsynchronisie-  
 rung **32**  
 Installieren  
 Arbeitsblatt **68**  
 herunterladen, IaaS-Installationsprogramm **81**  
 Konfigurieren der VMware vCloud Automation  
 Center Appliance **72**  
 Überlegungen zum Browser **20**  
 Integritätsprüfungen **66**  
 Interner Fehler, Hinzufügen eines XaaS-Endpo-  
 ints **147**

## J

Java-Anforderungen, für MSSQL-Datenbank **22**

## K

Kennwort, Einschränkungen **21**  
 Knoten-IDs **156**  
 Konfigurieren, vRealize Automation-Appli-  
 ance **73**  
 Kontoeinstellungen, festlegen **62**

## L

Lastausgleichsdienst, Zeitüberschreitung vor  
 Fertigstellung, ändern, Zeitüberschrei-  
 tungswert für Lastausgleichsdienst **137**  
 Lastausgleichsdienste  
 Integritätsprüfungen **66**  
 Konfigurieren **72**  
 Laufzeit-Authentifizierung **103**  
 Log Insight **129**

## M

Management-Agent  
 deinstallieren **37, 44**  
 Hintergrundinstallation **154**  
 installieren **37, 44**  
 Installieren **36, 44**  
 Management-Agent-SSL-Fingerabdruck, Su-  
 chen **36, 44**

Manager Service  
 Anforderungen **23**  
 Definition **65**  
 Installieren **94, 97**  
 Manager Service, vertrauenswürdiges Zertifi-  
 kat **68**  
 Mandanten, Konfigurieren des Standardmandan-  
 ten **129**  
 Master-Knoten fehlerhaft **142**  
 Minimalbereitstellung, Überblick über die Instal-  
 lation **13**  
 Minimalbereitstellungen, Installation mithilfe des  
 Installationsassistenten **35**  
 Minimalinstallation, Deinstallieren **135**  
 Model Manager  
 Ausführungsrichtlinien **16**  
 bearbeitbare Geschäftslogik **16**  
 Definition **65**  
 Fehlerbehebung bei Installationsfehlern **145**  
 sichere Mehrinstanzfähigkeit **16**  
 vereinheitlichtes Datenmodell **16**  
 Model Manager-Daten, Installieren **87, 88, 90,**  
**91**  
 Model Manager-Web **16**

## N

nach der Installation **129**

## O

OpenStack, DEM-Anforderungen **25**

## P

PEM-Dateien, Befehl zum Extrahieren **31**  
 PFX-Dateien, Konfigurieren eines vertrauens-  
 würdigen Zertifikats **68**  
 PowerShell, festlegen auf „RemoteSigned“ **105**  
 PowerVC, DEM-Anforderungen **25**  
 Protokolle  
 Fehlerbehebung **133**  
 IaaS **133**  
 sammeln **136**  
 Speicherorte **133**  
 Proxy **151**  
 Proxy-Agent, Deinstallation schlägt fehl **147**  
 Proxy-Agents, Installieren und Konfigurieren für  
 vSphere **106**

## R

RSA-Privatschlüssel, Befehl zum Extrahieren **31**

## S

Servieranforderungen, IaaS oder Windows Ser-  
 ver **22**  
 Servereinstellungen, festlegen **62**  
 Sicherheit  
 Drittanbietersoftware **32**

- IaaS-Zertifikate **59, 81**
- Kennwortsatz **31**
- Vertrauensstellungen **67**
- Zertifikate **30**
- Snapshots, Erstellen **40, 48**
- SQL, Anforderungen **21**
- SQL-Authentifizierung **103**
- SSL-Zertifikate, Extrahieren **31**
- Support-Paket, Erstellen **136**
- Systemfehlermeldung **141**
- Szenarien, Auswählen der Agent-Installation **106**

**U**

- Unternehmensbereitstellung, Installation mithilfe des Assistenten **43**

**V**

- vCloud Suite, Lizenzierung **7**
- VDI-Agent für XenDesktop, Installieren **116**
- Verkettete Zertifikate, Reihenfolge **30**
- Verteilte Bereitstellung
  - Deaktivieren nicht verwendeter Dienste **79**
  - Installation mithilfe des Assistenten **43**
  - Überblick über die Installation **13**
  - überprüfen **79**
- Verteilte IaaS-Installation **65**
- Verteilte Installation
  - Deinstallieren **135**
  - Übersicht **64**
- Vertrauenswürdige Zertifikat, Probleme **145**
- Virtualisierungs-Proxy-Agents **17**
- Visual Basic, Anforderungen bei Skripterstellung **123**
- Visual Basic-Skripterstellung
  - Installieren der EPI-Agents **123**
  - Installieren des EPI-Agents **122**
- VMware IaaS
  - Distributed Execution Manager **16**
  - Manager Service **16**
- VMware IaaS, Datenbank **16**
- VMware IaaS, Model Manager **16**
- VMware Identity Manager **151**
- VMware-IaaS, IaaS-Website **16**
- Voraussetzungen
  - Überlegungen zum Browser **20**
  - Überprüfen **61**
- Voraussetzungsprüfung, Ausführen im Installationsassistenten **39, 47**
- vRealize Appliance
  - Bereitstellen **33, 52**
  - Konfigurieren **55**
- vRealize Appliance-Cluster; Hinzufügen **78**
- vRealize Automation-Appliance, Bereitstellen **70**

- vRealize Automation-Appliances, Fehlerbehebung **140**
- vRealize Orchestrator, Verwendung externer Komponenten für High Availability-Bereitstellungen **64**
- vSphere-Agent
  - erforderliche Berechtigungen **107**
  - unterstützte Konfiguration für Gleichzeitigkeit **107**
- vSphere-Agents
  - Installieren **108**
  - Konfigurieren **111**
  - Vertrauenswürdige Zertifikat anfordern **111**
- vSphere-Proxy-Agents, Installieren und konfigurieren **106**

**W**

- WAPI, Installation schlägt fehl **144**
- Website-Komponente, Installieren **87, 88, 90, 91**
- Windows-Authentifizierung **103**
- WMI-Agents
  - Aktivieren von Remote-Anforderungen **125**
  - Installieren **126**

**X**

- XenDesktop
  - Installationsanforderungen **116**
  - Installieren des Agents **117**
  - Installieren des VDI-Agents **116**
- XenServer
  - Agent **112**
  - Proxy-Agent **112**
- XenServer-Agents, Installieren **112**
- XenServer-Hostname, Einstellung **117**

**Z**

- Zeiteinstellungen der virtuellen Appliances, mit dem Installationsassistenten **39, 47**
- Zeitsynchronisierung
  - Aktivieren auf Windows-Maschine **59**
  - Server **54, 77**
- Zertifikate
  - Vertrauensstellungen **67**
  - Wechseln von selbstsignierten Zertifikaten **129**
- Zertifikatnamenskonflikt **145**
- Zertifikatsketten, Reihenfolge **30**
- Zertifikatsvalidierung **143**