

Installing vRealize Automation

vRealize Automation 7.2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-002325-02

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

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

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

vRealize Automation Installation	7
Updated Information	9
1 vRealize Automation Installation Overview	11
vRealize Automation Installation Components	11
The vRealize Automation Appliance	12
Infrastructure as a Service	12
Deployment Type	14
Minimal vRealize Automation Deployments	15
Distributed vRealize Automation Deployments	16
Choosing Your Installation Method	17
2 Preparing for vRealize Automation Installation	19
Host Names and IP Addresses	19
Hardware and Virtual Machine Requirements	20
Browser Considerations	20
Password Considerations	21
Windows Server Requirements	21
IaaS Database Server Requirements	21
IaaS Web Service and Model Manager Server Requirements	22
IaaS Manager Service	23
Distributed Execution Manager Requirements	23
vRealize Automation Port Requirements	26
User Accounts and Credentials Required for Installation	28
Security	30
Certificates	30
Extracting Certificates and Private Keys	30
Security Passphrase	31
Third-Party Software	31
Time Synchronization	31
3 Installing vRealize Automation with the Installation Wizard	33
Deploy the vRealize Automation Appliance	33
Using the Installation Wizard for Minimal Deployments	35
Run the Installation Wizard for a Minimal Deployment	35
Installing the Management Agent	35
Synchronize Server Times	38
Run the Prerequisite Checker	38
Specify Minimal Deployment Parameters	39
Create Snapshots Before You Begin the Installation	39
Finish the Installation	39

	Address Installation Failures	40
	Set Up Credentials for Initial Content Configuration	40
	Using the Installation Wizard for Enterprise Deployments	41
	Run the Installation Wizard for an Enterprise Deployment	41
	Installing the Management Agent	42
	Synchronize Server Times	44
	Run the Prerequisite Checker	45
	Specify Enterprise Deployment Parameters	46
	Create Snapshots Before You Begin the Installation	46
	Finish the Installation	46
	Address Installation Failures	47
	Set Up Credentials for Initial Content Configuration	48
4	The Standard vRealize Automation Installation Interfaces	49
	Using the Standard Interfaces for Minimal Deployments	49
	Minimal Deployment Checklist	49
	Deploy and Configure the vRealize Automation Appliance	50
	Installing IaaS Components	55
	Using the Standard Interfaces for Distributed Deployments	60
	Distributed Deployment Checklist	60
	Distributed Installation Components	61
	Disabling Load Balancer Health Checks	62
	Certificate Trust Requirements in a Distributed Deployment	63
	Configure Web Component, Manager Service and DEM Host Certificate Trust	63
	Installation Worksheets	64
	Deploy the vRealize Automation Appliance	66
	Configuring Your Load Balancer	68
	Configuring Appliances for vRealize Automation	68
	Install the IaaS Components in a Distributed Configuration	74
	Installing vRealize Automation Agents	97
	Set the PowerShell Execution Policy to RemoteSigned	98
	Choosing the Agent Installation Scenario	98
	Agent Installation Location and Requirements	99
	Installing and Configuring the Proxy Agent for vSphere	99
	Installing the Proxy Agent for Hyper-V or XenServer	104
	Installing the VDI Agent for XenDesktop	108
	Installing the EPI Agent for Citrix	111
	Installing the EPI Agent for Visual Basic Scripting	114
	Installing the WMI Agent for Remote WMI Requests	117
5	vRealize Automation Post-Installation Tasks	121
	Configure Federal Information Processing Standard Compliant Encryption	121
	Replacing Self-Signed Certificates with Certificates Provided by an Authority	122
	Change the Master vRealize Automation Appliance Host Name	122
	Change a Replica vRealize Automation Appliance Host Name	123
	Installing the vRealize Log Insight Agent on IaaS Servers	124
	Configure Access to the Default Tenant	124

6	Troubleshooting a vRealize Automation Installation	127
	Default Log Locations	127
	Rolling Back a Failed Installation	128
	Roll Back a Minimal Installation	128
	Roll Back a Distributed Installation	129
	Create a vRealize Automation Support Bundle	130
	General Installation Troubleshooting	130
	Installation or Upgrade Fails with a Load Balancer Timeout Error	130
	Server Times Are Not Synchronized	131
	Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7	131
	Cannot Establish Trust Relationship for the SSL/TLS Secure Channel	132
	Connect to the Network Through a Proxy Server	132
	Console Steps for Initial Content Configuration	133
	Cannot Downgrade vRealize Automation Licenses	134
	Troubleshooting the vRealize Automation Appliance	134
	Installers Fail to Download	134
	Encryption.key File has Incorrect Permissions	134
	Identity Manager Fails to Start After Horizon-Workspace Restart	135
	Incorrect Appliance Role Assignments After Failover	136
	Failures After Promotion of Replica and Master Nodes	136
	Incorrect vRealize Automation Component Service Registrations	137
	Troubleshooting IaaS Components	138
	Validating Server Certificates for IaaS	138
	Credentials Error When Running the IaaS Installer	138
	Save Settings Warning Appears During IaaS Installation	139
	Website Server and Distributed Execution Managers Fail to Install	139
	IaaS Authentication Fails During IaaS Web and Model Management Installation	139
	Failed to Install Model Manager Data and Web Components	140
	IaaS Windows Servers Do Not Support FIPS	141
	Adding an XaaS Endpoint Causes an Internal Error	141
	Uninstalling a Proxy Agent Fails	142
	Machine Requests Fail When Remote Transactions Are Disabled	142
	Error in Manager Service Communication	143
	Email Customization Behavior Has Changed	143
	Troubleshooting Log-In Errors	144
	Attempts to Log In as the IaaS Administrator with Incorrect UPN Format Credentials Fails with No Explanation	144
	Log In Fails with High Availability	144
	Proxy Prevents VMware Identity Manager User Log In	145
7	Silent vRealize Automation Installation	147
	Perform a Silent vRealize Automation Installation	147
	Perform a Silent vRealize Automation Management Agent Installation	148
	Silent vRealize Automation Installation Answer File	149
	The vRealize Automation Installation Command Line	149
	vRealize Automation Installation Command Line Basics	150
	vRealize Automation Installation Command Names	150
	The vRealize Automation Installation API	151
	Convert Between vRealize Automation Silent Properties and JSON	152

Index 153

vRealize Automation Installation

vRealize Automation Installation explains how to install VMware vRealize™ Automation.

NOTE Not all features and capabilities of vRealize Automation are available in all editions. For a comparison of feature sets in each edition, see <https://www.vmware.com/products/vrealize-automation/>.

Intended Audience

This information is intended for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

Updated Information

The following table lists the changes to *Installing vRealize Automation* for this product release.

Revision	Description
EN-002325-02	<ul style="list-style-type: none">■ Added another restart in “Change the Master vRealize Automation Appliance Host Name,” on page 122 and “Change a Replica vRealize Automation Appliance Host Name,” on page 123.■ Added “Cannot Downgrade vRealize Automation Licenses,” on page 134.
EN-002325-01	Added Configure a Datastore Cluster permission to “vSphere Agent Requirements,” on page 99.
EN-002325-00	Initial document release.

vRealize Automation Installation Overview

1

You can install vRealize Automation through different means, each with varying levels of interactivity.

To install, you deploy a vRealize Automation appliance and then complete the bulk of the installation using one of the following options:

- A consolidated, browser-based Installation Wizard
- Separate browser-based appliance configuration, and separate Windows installations for IaaS server components
- A command line based, silent installer that accepts input from an answer properties file
- An installation REST API that accepts JSON formatted input

After installation, you start using vRealize Automation by customizing the environment and configuring one or more tenants, which sets up access to self-service provisioning and life-cycle management of cloud services.

If you installed earlier versions of vRealize Automation, note the following changes before you begin.

- This release of vRealize Automation introduces an installation API that uses a JSON formatted version of the silent installation settings.
See [“The vRealize Automation Installation API,”](#) on page 151.
- This release supports the changing of vRealize Automation appliance host names.
See [“Change the Master vRealize Automation Appliance Host Name,”](#) on page 122.
- This release of the vRealize Automation Installation Wizard introduces a post-installation option to migrate data from an older deployment.

This chapter includes the following topics:

- [“vRealize Automation Installation Components,”](#) on page 11
- [“Deployment Type,”](#) on page 14
- [“Choosing Your Installation Method,”](#) on page 17

vRealize Automation Installation Components

A typical vRealize Automation installation consists of a vRealize Automation appliance and one or more Windows servers that, taken together, provide vRealize Automation Infrastructure as a Service (IaaS).

The vRealize Automation Appliance

The vRealize Automation appliance is a preconfigured Linux virtual appliance. The vRealize Automation appliance is delivered as an open virtualization file that you deploy on existing virtualized infrastructure such as vSphere.

The vRealize Automation appliance performs several functions central to vRealize Automation.

- The appliance contains the server that hosts the vRealize Automation product portal, where users log in to access self-service provisioning and management of cloud services.
- The appliance manages single sign-on (SSO) for user authorization and authentication.
- The appliance server hosts a management interface for vRealize Automation appliance settings.
- The appliance includes a preconfigured PostgreSQL database used for internal vRealize Automation appliance operations.

In large deployments with redundant appliances, the secondary appliance databases serve as replicas to provide high availability.

- The appliance includes a preconfigured instance of vRealize Orchestrator. vRealize Automation uses vRealize Orchestrator workflows and actions to extend its capabilities.

The embedded instance of vRealize Orchestrator is now recommended. In older deployments or special cases, however, users might connect vRealize Automation to an external vRealize Orchestrator instead.

- The appliance contains the downloadable Management Agent installer. All Windows servers that make up your vRealize Automation IaaS must install the Management Agent.

The Management Agent registers IaaS Windows servers with the vRealize Automation appliance, automates the installation and management of IaaS components, and collects support and telemetry information.

Infrastructure as a Service

vRealize Automation IaaS consists of one or more Windows servers that work together to model and provision systems in private, public, or hybrid cloud infrastructures.

You install vRealize Automation IaaS components on one or more virtual or physical Windows servers. After installation, IaaS operations appear under the Infrastructure tab in the product interface.

IaaS consists of the following components, which can be installed together or separately, depending on deployment size.

Web Server

The IaaS Web server provides infrastructure administration and service authoring to the vRealize Automation product interface. The Web server component communicates with the Manager Service, which provides updates from the Distributed Execution Manager (DEM), SQL Server database, and agents.

Model Manager

vRealize Automation uses models to facilitate integration with external systems and databases. The models implement business logic used by the DEM.

The Model Manager provides services and utilities for persisting, versioning, securing, and distributing model elements. Model Manager is hosted on one of the IaaS Web servers and communicates with DEMs, the SQL Server database, and the product interface Web site.

Manager Service

The Manager Service is a Windows service that coordinates communication between IaaS DEMs, the SQL Server database, agents, and SMTP.

IaaS requires that only one Windows machine actively run the Manager Service. For backup or high availability, you may deploy additional Windows machines where you manually start the Manager Service if the active service stops.

IMPORTANT Simultaneously running an active Manager Service on multiple IaaS Windows servers makes vRealize Automation unusable.

The Manager Service communicates with the Web server through the Model Manager and must be run under a domain account with administrator privileges on all IaaS Windows servers.

SQL Server Database

IaaS uses a Microsoft SQL Server database to maintain information about the machines it manages, plus its own elements and policies. Most users allow vRealize Automation to create the database during installation. Alternatively, you may create the database separately if site policies require it.

Distributed Execution Manager

The IaaS DEM component runs the business logic of custom models, interacting with the IaaS SQL Server database, and with external databases and systems. A common approach is to install DEMs on the IaaS Windows server that hosts the active Manager Service, but it is not required.

Each DEM instance acts as a worker or orchestrator. The roles can be installed on the same or separate servers.

DEM Worker—A DEM worker has one function, to run workflows. Multiple DEM workers increase capacity and can be installed on the same or separate servers.

DEM Orchestrator—A DEM orchestrator performs the following oversight functions.

- Monitors DEM workers. If a worker stops or loses its connection to Model Manager, the DEM orchestrator moves the workflows to another DEM worker.
- Schedules workflows by creating new workflow instances at the scheduled time.
- Ensures that only one instance of a scheduled workflow is running at a given time.
- Preprocesses workflows before they run. Preprocessing includes checking preconditions for workflows and creating the workflow execution history.

The active DEM orchestrator needs a strong network connection to the Model Manager host. In large deployments with multiple DEM orchestrators on separate servers, the secondary orchestrators serve as backups by monitoring the active DEM orchestrator, and provide redundancy and failover if a problem occurs with the active DEM orchestrator. For this kind of failover configuration, you might consider installing the active DEM orchestrator with the active Manager Service host, and secondary DEM orchestrators with the standby Manager Service hosts.

Agents

vRealize Automation IaaS uses agents to integrate with external systems and to manage information among vRealize Automation components.

A common approach is to install vRealize Automation agents on the IaaS Windows server that hosts the active Manager Service, but it is not required. Multiple agents increase capacity and can be installed on the same or separate servers.

Virtualization Proxy Agents

vRealize Automation creates and manages virtual machines on virtualization hosts. Virtualization proxy agents send commands to, and collect data from, vSphere ESX Server, XenServer, and Hyper-V hosts, and the virtual machines provisioned on them.

A virtualization proxy agent has the following characteristics.

- Typically requires administrator privileges on the virtualization platform that it manages.
- Communicates with the IaaS Manager Service.
- Is installed separately and has its own configuration file.

Most vRealize Automation deployments install the vSphere proxy agent. You might install other proxy agents depending on the virtualization resources in use at your site.

Virtual Desktop Integration Agents

Virtual desktop integration (VDI) PowerShell agents allow vRealize Automation to integrate with external virtual desktop systems. VDI agents require administrator privileges on the external systems.

You can register virtual machines provisioned by vRealize Automation with XenDesktop on a Citrix Desktop Delivery Controller (DDC), which allows the user to access the XenDesktop Web interface from vRealize Automation.

External Provisioning Integration Agents

External provisioning integration (EPI) PowerShell agents allow vRealize Automation to integrate external systems into the machine provisioning process.

For example, integration with Citrix Provisioning Server enables provisioning of machines by on-demand disk streaming, and an EPI agent allows you to run Visual Basic scripts as extra steps during the provisioning process.

EPI agents require administrator privileges on the external systems with which they interact.

Windows Management Instrumentation Agent

The vRealize Automation Windows Management Instrumentation (WMI) agent enhances your ability to monitor and control Windows system information, and allows you to manage remote Windows servers from a central location. The WMI agent also enables collection of data from Windows servers that vRealize Automation manages.

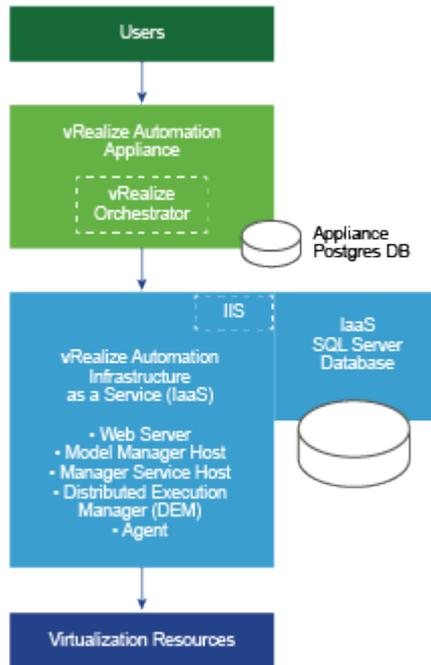
Deployment Type

You can install vRealize Automation as a minimal deployment for proof of concept or development work, or in a distributed configuration suitable for medium to large production workloads.

Minimal vRealize Automation Deployments

Minimal deployments include one vRealize Automation appliance and one Windows server that hosts the IaaS components. In a minimal deployment, the vRealize Automation SQL Server database can be on the same IaaS Windows server with the IaaS components, or on a separate Windows server.

Figure 1-1. Minimal vRealize Automation Deployment

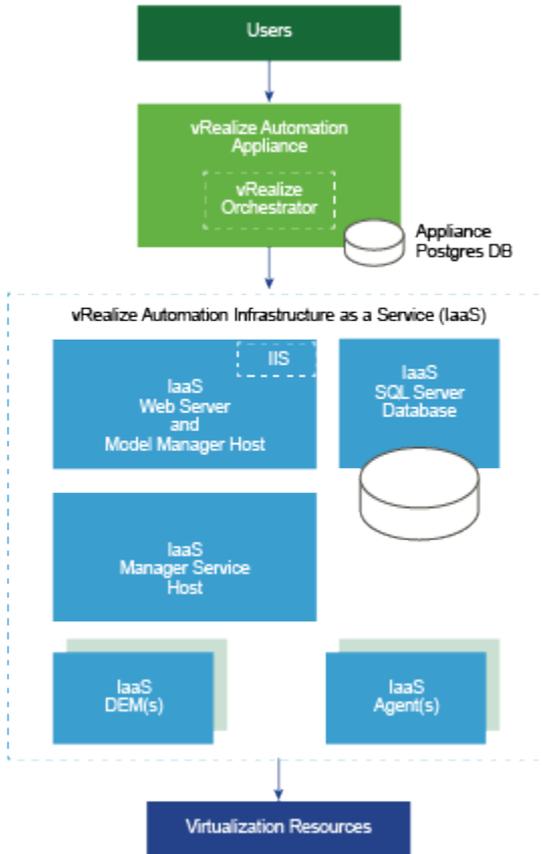


NOTE The vRealize Automation documentation includes a complete, sample minimal deployment scenario that walks you through installation and how to start using the product for proof of concept. See *Installing and Configuring vRealize Automation for the Rainpole Scenario*.

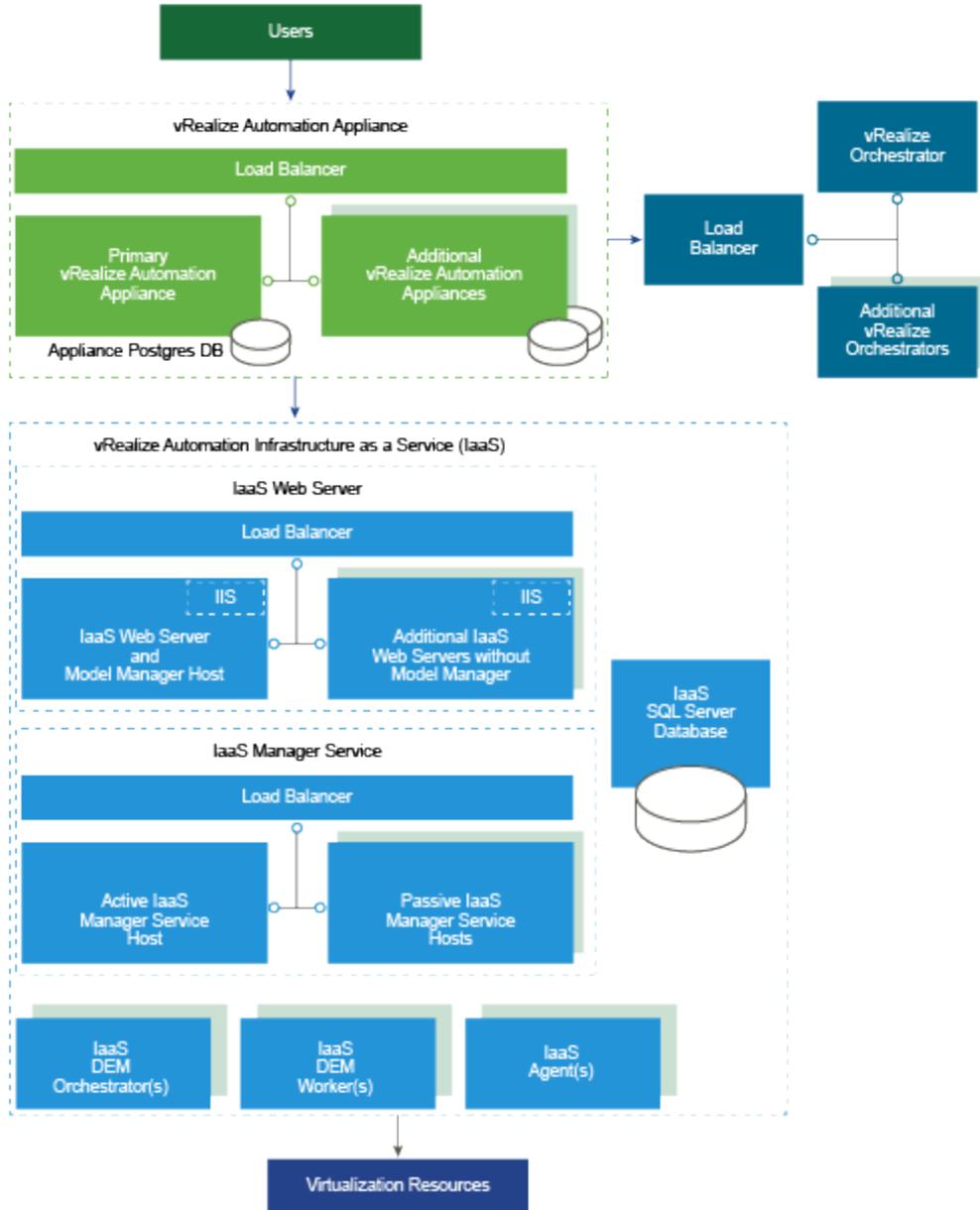
Distributed vRealize Automation Deployments

Distributed, enterprise deployments can be of varying size. A basic distributed deployment might improve vRealize Automation simply by hosting IaaS components on separate Windows servers as shown in the following figure.

Figure 1-2. Distributed vRealize Automation Deployment



Many production deployments go even further, with redundant appliances, redundant servers, and load balancing for even more capacity. Large, distributed deployments provide for better scale, high availability, and disaster recovery. Note that the embedded instance of vRealize Orchestrator is now recommended, but you might see vRealize Automation connected to an external vRealize Orchestrator in older deployments.

Figure 1-3. Large Distributed and Load Balanced vRealize Automation Deployment

For more information about scalability and high availability, see the *vRealize Automation Reference Architecture* guide.

Choosing Your Installation Method

The consolidated vRealize Automation Installation Wizard is your primary tool for new vRealize Automation installations. Alternatively, you might want to perform the manual, separate installation processes in some cases.

- The Installation Wizard provides a simple and fast way to install, from minimal deployments to distributed enterprise deployments with or without load balancers. Most users run the Installation Wizard.

- You need the manual installation steps if you want to expand a vRealize Automation deployment or if the Installation Wizard stopped for any reason.

Once you begin a manual installation, you cannot go back and run the Installation Wizard.

Preparing for vRealize Automation Installation

2

System Administrators install vRealize Automation into their existing virtualization environments. Before you begin an installation, prepare the deployment environment to meet system requirements.

This chapter includes the following topics:

- [“Host Names and IP Addresses,”](#) on page 19
- [“Hardware and Virtual Machine Requirements,”](#) on page 20
- [“Browser Considerations,”](#) on page 20
- [“Password Considerations,”](#) on page 21
- [“Windows Server Requirements,”](#) on page 21
- [“vRealize Automation Port Requirements,”](#) on page 26
- [“User Accounts and Credentials Required for Installation,”](#) on page 28
- [“Security,”](#) on page 30
- [“Time Synchronization,”](#) on page 31

Host Names and IP Addresses

vRealize Automation requires that you name the hosts in your installation according to certain requirements.

- All vRealize Automation machines in your installation must be able to resolve each other by fully qualified domain name (FQDN).

While performing the installation, always enter the FQDN when identifying or selecting a machine. Do not enter IP addresses.

- In addition to the FQDN requirement, Windows machines that host the Model Manager Web service, Manager Service, and Microsoft SQL Server database must be able to resolve each other by Windows Internet Name Service (WINS) name.

Configure your Domain Name System (DNS) to resolve these short WINS host names.

- Preplan domain and machine naming so that vRealize Automation machines will begin and end with alphabet (a-z) or digit (0-9) characters, and will only contain alphabet, digit, or hyphen (-) characters. The underscore character (_) must not appear in the host name or anywhere in the FQDN.

For more information about allowable names, review the host name specifications from the Internet Engineering Task Force. See www.ietf.org.

- In general, you should expect to keep the host names and FQDNs that you planned for vRealize Automation systems. You can change a vRealize Automation appliance host name after installation, but changing other vRealize Automation host names makes vRealize Automation unusable.
- A best practice is to reserve and use static IP addresses for all vRealize Automation appliances and IaaS Windows servers. vRealize Automation supports DHCP, but static IP addresses are recommended for long-term deployments such as production environments.
 - You apply an IP address to the vRealize Automation appliance during OVF or OVA deployment.
 - For the IaaS Windows servers, you follow the usual operating system process. Set the IP address before installing vRealize Automation IaaS.

Hardware and Virtual Machine Requirements

Your deployment must meet minimum system resources to install virtual appliances and minimum hardware requirements to install IaaS components on the Windows Server.

For operating system and high-level environment requirements, including information about supported browsers and operating systems, see the *vRealize Automation Support Matrix*.

The Hardware Requirements table shows the minimum configuration requirements for deployment of virtual appliances and installation of IaaS components. Appliances are pre-configured virtual machines that you add to your vCenter Server or ESXi inventory. IaaS components are installed on physical or virtual Windows 2008 R2 SP1, or Windows 2012 R2 servers.

An Active Directory is considered small when there are up to 25,000 users in the OU to be synced in the ID Store configuration. An Active Directory is considered large when there are more than 25,000 users in the OU.

Table 2-1. Hardware Requirements

vRealize Automation appliance for Small Active Directories	vRealize Automation appliance for Large Active Directories	IaaS Components (Windows Server).
<ul style="list-style-type: none"> ■ 4 CPUs ■ 18 GB memory ■ 60 GB disk storage 	<ul style="list-style-type: none"> ■ 4 CPUs ■ 22 GB memory ■ 60 GB disk storage 	<ul style="list-style-type: none"> ■ 2 CPUs ■ 8 GB memory ■ 30 GB disk storage <p>Additional resources are required when you are include an SQL Server on a Windows host.</p>

Browser Considerations

Some restrictions exist for browser use with vRealize Automation.

- Multiple browser windows and tabs are not supported. vRealize Automation supports one session per user.
- VMware Remote Consoles provisioned on vSphere support a subset of vRealize Automation-supported browsers.

For operating system and high-level environment requirements, including information about supported browsers and operating systems, see the *vRealize Automation Support Matrix*.

Password Considerations

Character restrictions apply to some passwords.

The VMware vRealize™ Automation administrator password cannot contain a trailing "=" character. Such passwords are accepted when you assign them, but result in errors when you perform operations such as saving endpoints.

Windows Server Requirements

The virtual or physical Windows machine that hosts the IaaS components must meet configuration requirements for the IaaS database, the IaaS server components, the IaaS Manager Service, and Distributed Execution Managers.

The Installation Wizard runs a vRealize Automation prerequisite checker on all IaaS Windows servers to ensure that they meet the configuration necessary for installation. In addition to the prerequisite checker, address the following prerequisites separately.

- As a best practice, place all IaaS Windows servers in the same domain.
- Create or identify a domain account to use for installation, one that has administrator privileges on all IaaS Windows servers.

IaaS Database Server Requirements

The Windows server that hosts the vRealize Automation IaaS SQL Server database must meet certain prerequisites.

The requirements apply whether you run the Installation Wizard or the legacy `setup_vrealize-automation-appliance-URL.exe` installer and select the database role for installation. The prerequisites also apply if you separately create an empty SQL Server database for use with IaaS.

- Use a supported SQL Server version from the *vRealize Automation Support Matrix*.
- Enable TCP/IP protocol for SQL Server.
- Enable the Distributed Transaction Coordinator (DTC) service on all IaaS Windows servers and the machine that hosts SQL Server. IaaS uses DTC for database transactions and actions such as workflow creation.

NOTE If you clone a machine to make an IaaS Windows server, install DTC on the clone after cloning. If you clone a machine that already has DTC, its unique identifier is copied to the clone, which causes communication to fail. See [“Error in Manager Service Communication,”](#) on page 143.

For more about DTC enablement, see [VMware Knowledge Base article 2038943](#).

- Open ports between all IaaS Windows servers and the machine that hosts SQL Server. See [“vRealize Automation Port Requirements,”](#) on page 26.

Alternatively, if site policies allow, you may disable firewalls between IaaS Windows servers and SQL Server.

- This release of vRealize Automation does not support SQL Server 2016 130 compatibility mode. If you separately create an empty SQL Server 2016 database for use with IaaS, use 100 or 120 compatibility mode.

If you create the database through a vRealize Automation installer, compatibility is already configured.

- AlwaysOn Availability Group (AAG) is only supported with SQL Server 2016.

IaaS Web Service and Model Manager Server Requirements

Your environment must meet software and configuration prerequisites that support installation of the IaaS server components.

Environment and Database Requirements for IaaS

Your host configuration and MS SQL database must meet the following requirements.

Table 2-2. IaaS Requirements

Area	Requirements
Host Configuration	<p>The following components must be installed on the host before installing IaaS:</p> <ul style="list-style-type: none"> ■ Microsoft .NET Framework 4.5.2 or later. ■ Microsoft PowerShell 2.0 (included with Windows Server 2008 R2 SP1 and later) or Microsoft PowerShell 3.0 on Windows Server 2012 R2. ■ Microsoft Internet Information Services 7.5. ■ Java must be installed on the machine running the primary Web component to support deployment of the MS SQL database during installation.
Microsoft SQL Database Requirements	<p>The SQL database can reside on one of your IaaS Windows servers, or a separate host.</p> <p>If the SQL database is on one of your IaaS Windows servers, configure the following Java requirements.</p> <ul style="list-style-type: none"> ■ Install 64-bit Java 1.8 or later. Do not use 32-bit. ■ Set the JAVA_HOME environment variable to the Java installation folder. ■ Verify that %JAVA_HOME%\bin\java.exe is available.

Microsoft Internet Information Services Requirements

Configure Internet Information Services (IIS) to meet the following requirements.

In addition to the configuration settings, avoid hosting additional Web sites in IIS on the IaaS Web server host. vRealize Automation sets the binding on its communication port to all unassigned IP addresses, making no additional bindings possible. The default vRealize Automation communication port is 443.

Table 2-3. Required Configuration for Microsoft Internet Information Services

IIS Component	Setting
Internet Information Services (IIS) modules installed	<ul style="list-style-type: none"> ■ WindowsAuthentication ■ StaticContent ■ DefaultDocument ■ ASPNET 4.5 ■ ISAPIExtensions ■ ISAPIFilter
IIS Authentication settings	<ul style="list-style-type: none"> ■ Windows Authentication enabled ■ AnonymousAuthentication disabled ■ Negotiate Provider enabled ■ NTLM Provider enabled ■ Windows Authentication Kernel Mode enabled ■ Windows Authentication Extended Protection disabled ■ For certificates using SHA512, TLS1.2 must be disabled on Windows 2012 or Windows 2012 R2 servers
IIS Windows Process Activation Service roles	<ul style="list-style-type: none"> ■ ConfigurationApi ■ NetEnvironment ■ ProcessModel ■ WcfActivation (Windows 2008 only) ■ HttpActivation ■ NonHttpActivation

IaaS Manager Service

Your environment must meet some general requirements that support the installation of the IaaS Manager Service.

- Microsoft .NET Framework 4.5.2 is installed.
- Microsoft PowerShell 2.0, 3.0, or 4.0. Some vRealize Automation upgrades or migrations might require you to install an older or newer PowerShell version, in addition to the one that you are currently running.
- SecondaryLogOnService is running.
- No firewalls can exist between DEM host and Windows Server. For port information, see [“vRealize Automation Port Requirements,”](#) on page 26.
- IIS is installed and configured.

Distributed Execution Manager Requirements

Your environment must meet some general requirements that support the installation of Distributed Execution Managers (DEMs).

- Microsoft .NET Framework 4.5.2 is installed.
- Microsoft PowerShell 2.0, 3.0, or 4.0. Some vRealize Automation upgrades or migrations might require you to install an older or newer PowerShell version, in addition to the one that you are currently running.
- SecondaryLogOnService is running.

- No firewalls between DEM host and the Windows server, or ports opened as described in “[vRealize Automation Port Requirements](#),” on page 26.

Servers that host DEM Worker instances might have additional requirements depending on the provisioning resources that they interact with.

Amazon Web Services EC2 Requirements

A vRealize Automation IaaS Windows server communicates with and collects data from an Amazon EC2 account.

When you use Amazon Web Services (AWS) for provisioning, the IaaS Windows servers that host the DEM workers must meet the following requirements.

- DEM worker hosts must have Internet access.
- If the DEM worker hosts are behind a firewall, HTTPS traffic must be allowed to and from `aws.amazon.com` as well as the URLs for EC2 regions that your AWS accounts have access to, such as `ec2.us-east-1.amazonaws.com` for the US East region.

Each URL resolves to a range of IP addresses, so you might need to use a tool, such as the one available from the Network Solutions Web site, to list and configure these IP addresses.

- If the DEM worker hosts reach the Internet through a proxy server, the DEM service must be running under credentials that can authenticate to the proxy server.

Openstack and PowerVC Requirements

The machines on which you install your DEMs must meet certain requirements to communicate with and collect data from your Openstack or PowerVC instance.

Table 2-4. DEM Host Requirements

Your Installation	Requirements
All	<p>In Windows Registry, enable TLS v1.2 support for .NET framework. For example:</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>In Windows Registry, enable TLS v1.2 protocol. For example:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
Self-signed certificates on your infrastructure endpoint host	<p>If your PowerVC or Openstack instance is not using trusted certificates, import the SSL certificate from your PowerVC or Openstack instance into the Trusted Root Certificate Authorities store on each IaaS Windows server where you intend to install a vRealize Automation DEM.</p>

Red Hat Enterprise Virtualization KVM (RHEV) Requirements

When you use Red Hat Enterprise Virtualization for provisioning the IaaS Windows server communicates with and collects data from that account.

Your environment must meet the following Red Hat Enterprise requirements.

- Each KVM (RHEV) environment must be joined to the domain containing the IaaS server.
- The credentials used to manage the endpoint representing a KVM (RHEV) environment must have Administrator privileges on the RHEV environment. These credentials must also have sufficient privileges to create objects on the hosts within the environment.

SCVMM Requirements

A DEM Worker that manages virtual machines through SCVMM must be installed on a host where the SCVMM console is already installed.

A best practice is to install the SCVMM console on a separate DEM Worker machine. In addition, verify that the following requirements have been met.

- The DEM worker must have access to the SCVMM PowerShell module installed with the console.

- The PowerShell Execution Policy must be set to RemoteSigned or Unrestricted.

To verify the PowerShell Execution Policy, enter one of the following commands at the PowerShell command prompt.

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

- If all DEM Workers within the instance are not on machines that meet these requirements, use Skill commands to direct SCVMM-related workflows to DEM Workers that are.

The following additional requirements apply to SCVMM.

- This release supports SCVMM 2012 R2, which requires PowerShell 3 or later.
- Install the SCVMM console before you install vRealize Automation DEM Workers that consume SCVMM work items.

If you install the DEM Worker before the SCVMM console, you see log errors similar to the following example.

```
Workflow 'ScvmmEndpointDataCollection' failed with the following exception: The term 'Get-
VMMServer' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
```

To correct the problem, verify that the SCVMM console is installed, and restart the DEM Worker service.

- Each SCVMM instance must be joined to the domain containing the server.
 - The credentials used to manage the endpoint representing an SCVMM instance must have administrator privileges on the SCVMM server.
- The credentials must also have administrator privileges on the Hyper-V servers within the instance.
- Hyper-V servers within an SCVMM instance to be managed must be Windows 2008 R2 SP1 Servers with Hyper-V installed. The processor must be equipped with the necessary virtualization extensions .NET Framework 4.5.2 or later must be installed and Windows Management Instrumentation (WMI) must be enabled.
 - To provision machines on an SCVMM resource, you must add a user in at least one security role within the SCVMM instance.
 - To provision a Generation-2 machine on an SCVMM 2012 R2 resource, you must add the following properties in the blueprint.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

Generation-2 blueprints should have an existing data-collected virtualHardDisk (vHDX) in the blueprint build information page. Having it blank causes Generation-2 provisioning to fail.

For more information, see [“Configure the DEM to Connect to SCVMM at a Different Installation Path,”](#) on page 94.

For additional information about preparing your SCVMM environment, see *Configuring vRealize Automation*.

vRealize Automation Port Requirements

vRealize Automation uses designated ports for communication and data access.

Although vRealize Automation uses only port 443 for communication, there might be other ports to open on the system. Because open, unsecured ports might present security vulnerabilities, verify that only ports required by your business applications are open.

vRealize Automation Appliance

The following ports are used by the vRealize Automation appliance.

Table 2-5. Incoming Ports for the vRealize Automation appliance

Port	Protocol	Comments
22	TCP	Optional. Access for SSH sessions
80	TCP	Optional. Redirects to 443
111	TCP, UDP	RPC
443	TCP	Access to the vRealize Automation console and API calls
443	TCP	Access for machines to download the guest agent and software bootstrap agent
5480	TCP	Access to the virtual appliance Web management interface
5480	TCP	Used by the Management Agent
5488, 5489	TCP	Internally used by the vRealize Automation appliance for updates
4369, 25672,5671,5672	TCP	RabbitMQ messaging
8230, 8280, 8281	TCP	Internal vRealize Orchestrator instance.
8444	TCP	Console proxy communication for vSphere VMware Remote Console connections.

Table 2-6. Outgoing Ports for the vRealize Automation appliance

Port	Protocol	Comments
25, 587	TCP, UDP	SMTP for sending outbound notification emails
53	TCP, UDP	DNS
67, 68, 546, 547	TCP, UDP	DHCP
80	TCP	Optional. For fetching software updates. Updates can be downloaded separately and applied
110, 995	TCP, UDP	POP for receiving inbound notification emails
143, 993	TCP, UDP	IMAP for receiving inbound notification emails
123	TCP, UDP	Optional. For connecting directly to NTP instead of using host time
443	TCP	Communication with IaaS Manager Service and infrastructure endpoint hosts over HTTPS
443	TCP	Communication with the software bootstrap agent over HTTPS
902	TCP	ESXi network file copy operations and VMware Remote Console connections.
5050	TCP	Optional. For communicating with vRealize Business.
5432	TCP, UDP	Optional. For communicating with an Appliance Database
8281	TCP	Optional. For communicating with an external vRealize Orchestrator instance

Other ports might be required by specific vRealize Orchestrator plug-ins that communicate with external systems. See the documentation for the vRealize Orchestrator plug-in.

Infrastructure as a Service

The ports in the tables Incoming Ports for Infrastructure as a Service Components and Outgoing Ports for Infrastructure as a Service must be available for use by the IaaS Windows Server.

Table 2-7. Incoming Ports for Infrastructure as a Service Components

Component	Port	Protocol	Comments
Manager Service	443	TCP	Communication with IaaS components and vRealize Automation appliance over HTTPS
vRealize Automation appliance	443	TCP	Communication with IaaS components and vRealize Automation appliance over HTTPS
Infrastructure Endpoint Hosts	443	TCP	Communication with IaaS components and vRealize Automation appliance over HTTPS. Typically, 443 is the default communication port for virtual and cloud infrastructure endpoint hosts, but refer to the documentation provided by your infrastructure hosts for a full list of default and required ports
SQL Server instance	1433	TCP	MSSQL

Table 2-8. Outgoing Ports for Infrastructure as a Service Components

Component	Port	Protocol	Comments
All	53	TCP, UDP	DNS
All	67, 68, 546, 547	TCP, UDP	DHCP
All	123	TCP, UDP	Optional. NTP
Manager Service	443	TCP	Communication with vRealize Automation appliance over HTTPS
Distributed Execution Managers	443	TCP	Communication with Manager Service over HTTPS
Proxy agents	443	TCP	Communication with Manager Service and infrastructure endpoint hosts over HTTPS
Management Agent	443	TCP	Communication with the vRealize Automation appliance
Guest agent Software bootstrap agent	443	TCP	Communication with Manager Service over HTTPS
Manager Service Website	1433	TCP	MSSQL
All	5480	TCP	Communication with the vRealize Automation appliance.

Microsoft Distributed Transaction Coordinator Service

In addition to verifying that the ports listed in the previous tables are free for use, you must enable Microsoft Distributed Transaction Coordinator Service (MS DTC) communication between all servers in the deployment. MS DTC requires the use of port 135 over TCP and a random port between 1024 and 65535.

The Prerequisite Checker validates whether MS DTC is running and that the required ports are open.

User Accounts and Credentials Required for Installation

You must verify that you have the roles and credentials to install vRealize Automation components.

vCenter Service Account

If you plan to use a vSphere endpoint, you need a domain or local account that has the appropriate level of access configured in vCenter.

Virtual Appliance Installation

To deploy the vRealize Automation appliance, you must have the appropriate privileges on the deployment platform (for example, vSphere administrator credentials).

During the deployment process, you specify the password for the virtual appliance administrator account. This account provides access to the vRealize Automation appliance management console from which you configure and administer the virtual appliances.

IaaS Installation

Before installing IaaS components, add the user under which you plan to execute the IaaS installation programs to the Administrator group on the installation host.

IaaS Database Credentials

You can create the database during product installation or create it manually in the SQL server.

When you create or populate an MS SQL database through vRealize Automation, either with the Installation Wizard or through the management console, the following requirements apply:

- If you use the **Use Windows Authentication** option, the **sysadmin** role in SQL Server must be granted to the user executing the Management Agent on the primary IaaS web server to create and alter the size of the database.
- If you do not select **Use Windows Authentication**, the **sysadmin** role in SQL Server must be also be granted to the user executing the Management Agent on the primary IaaS web server. The credentials are used at runtime.
- If you populate a pre-created database through vRealize Automation, the user credentials you provide (either the current Windows user or the specified SQL user) need only **dbo** privileges for the IaaS database.

NOTE vRealize Automation users also require the correct level of Windows authentication access to log in and use vRealize Automation.

IaaS Service User Credentials

IaaS installs several Windows services that share a single service user.

The following requirements apply to the service user for IaaS services:

- The user must be a domain user.
- The user must have local Administrator privileges on all hosts on which the Manager Service or Web site component is installed. Do not do a workgroup installation.
- The user is configured with **Log on as a service** privileges. This privilege ensures that the Manager Service starts and generates log files.
- The user must have **dbo** privileges for the IaaS database. If you use the installer to create the database, ensure that the service user login is added to SQL Server prior to running the installer. The installer grants the service user **dbo** privileges after creating the database.
- The installer is run under the account that runs the Management Agent on the primary Web server. If you want to use the installer to create an MS SQL database during installation, you must have the **sysadmin** role enabled under MS SQL. This is not a requirement if you choose to use a pre-created empty database.
- The domain user account that you plan to use as the IIS application pool identity for the Model Manager Web Service is configured with **Log on as batch job** privileges.

Model Manager Server Specifications

Specify the Model Manager server name by using a fully qualified domain name (FQDN). Do not use an IP address to specify the server.

Security

vRealize Automation uses SSL to ensure secure communication among components. Passphrases are used for secure database storage.

For more information see [“Certificate Trust Requirements in a Distributed Deployment,”](#) on page 63.

Certificates

vRealize Automation uses SSL certificates for secure communication among IaaS components and instances of the vRealize Automation appliance. The appliances and the Windows installation machines exchange these certificates to establish a trusted connection. You can obtain certificates from an internal or external certificate authority, or generate self-signed certificates during the deployment process for each component.

For important information about troubleshooting, support, and trust requirements for certificates, see [VMware Knowledge Base article 2106583](#).

You can update or replace certificates after deployment. For example, a certificate may expire or you may choose to use self-signed certificates during your initial deployment, but then obtain certificates from a trusted authority before going live with your vRealize Automation implementation.

Table 2-9. Certificate Implementations

Component	Minimal Deployment (non-production)	Distributed Deployment (production-ready)
vRealize Automation Appliance	Generate a self-signed certificate during appliance configuration.	For each appliance cluster, you can use a certificate from an internal or external certificate authority. Multi-use and wildcard certificates are supported.
IaaS Components	During installation, accept the generated self-signed certificates or select certificate suppression.	Obtain a multi-use certificate, such as a Subject Alternative Name (SAN) certificate, from an internal or external certificate authority that your Web client trusts.

Certificate Chains

If you use certificate chains, specify the certificates in the following order.

- Client/server certificate signed by the intermediate CA certificate
- One or more intermediate certificates
- A root CA certificate

Include the BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate when you import certificates.

Extracting Certificates and Private Keys

Certificates that you use with the virtual appliances must be in the PEM file format.

The examples in the following table use Gnu openssl commands to extract the certificate information you need to configure the virtual appliances.

Table 2-10. Sample Certificate Values and Commands (openssl)

Certificate Authority Provides	Command	Virtual Appliance Entries
RSA Private Key	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -nocerts -out key.pem</code>	RSA Private Key
PEM File	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Certificate Chain
(Optional) Pass Phrase	n/a	Pass Phrase

Security Passphrase

vRealize Automation uses security passphrases for database security. A passphrase is a series of words used to create a phrase that generates the encryption key that protects data while at rest in the database.

Follow these guidelines when creating a security passphrase for the first time.

- Use the same passphrase across the entire installation to ensure that each component has the same encryption key.
- Use a phrase that is greater than eight characters long.
- Include uppercase, lowercase and numeric characters, and symbols.
- Memorize the passphrase or keep it in a safe place. The passphrase is required to restore database information in the event of a system failure or to add components after initial installation. Without the passphrase, you cannot restore successfully.

Third-Party Software

Some components of vRealize Automation depend on third-party software, including Microsoft Windows and SQL Server. To guard against security vulnerabilities in third-party products, ensure that your software is up-to-date with the latest patches from the vendor.

Time Synchronization

A system administrator must set up accurate timekeeping as part of the vRealize Automation installation.

Installation fails if time synchronization is set up incorrectly.

Timekeeping must be consistent and synchronized across the vRealize Automation appliance and Windows servers. By using the same timekeeping method for each component, you can ensure this consistency.

For virtual machines, you can use the following methods:

- Configuration by using Network Time Protocol (directly).
- Configuration by using Network Time Protocol through ESXi with VMware Tools. You must have NTP set up on the ESXi.

For more about timekeeping on Windows, see [VMware Knowledge Base article 1318](#).

Installing vRealize Automation with the Installation Wizard

3

The vRealize Automation Installation Wizard provides a simple and fast way to install minimal or enterprise deployments.

Before you launch the wizard, you deploy a vRealize Automation appliance and configure IaaS Windows servers to meet prerequisites. The Installation Wizard appears the first time you log in to the newly deployed vRealize Automation appliance.

- To stop the wizard and return later, click **Logout**.
- To disable the wizard, click **Cancel**, or log out and begin manual installation through the standard interfaces.

The wizard is your primary tool for new vRealize Automation installations. If you want to expand an existing vRealize Automation deployment after running the wizard, see the procedures in [Chapter 4, “The Standard vRealize Automation Installation Interfaces,”](#) on page 49.

This chapter includes the following topics:

- [“Deploy the vRealize Automation Appliance,”](#) on page 33
- [“Using the Installation Wizard for Minimal Deployments,”](#) on page 35
- [“Using the Installation Wizard for Enterprise Deployments,”](#) on page 41

Deploy the vRealize Automation Appliance

To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.

Some restrictions apply to the root password you create for the vRealize Automation administrator.

Prerequisites

- Download the vRealize Automation appliance from the VMware Web site.
- Log in to the vSphere client as a user with system administrator privileges.

Procedure

- 1 Select **File > Deploy OVF Template** from the vSphere client.
- 2 Browse to the vRealize Automation appliance file you downloaded and click **Open**.
- 3 Click **Next**.
- 4 Click **Next** on the OVF Template Details page.
- 5 Accept the license agreement and click **Next**.

- 6 Enter a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.
- 7 Follow the prompts until the Disk Format page appears.
- 8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.
- 9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

- 10 Configure the values on the Properties page.
 - a Enter the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.
 - b Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

This value is used to set the initial status of the SSH service in the appliance. If you are installing with the Installation Wizard, enable this before you begin the wizard. You can change this setting from the appliance management console after installation.
 - c Enter the fully qualified domain name of the virtual machine in the **Hostname** text box.
 - d Configure the networking properties.
- 11 Click **Next**.
- 12 Depending on your deployment, vCenter, and DNS configuration, select one of the following ways of finishing OVA deployment and powering up the vRealize Automation appliance.
 - If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.
 - a Select **Power on after deployment** and click **Finish**.
 - b After the file finishes deploying into vCenter, click **Close**.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
 - a After the file finishes deploying into vCenter, click **Close**.
 - b Power on the vRealize Automation appliance.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - d Verify that you can ping the DNS for the vRealize Automation appliance. If you cannot ping the DNS, restart the virtual machine.
 - e Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed the vRealize Automation appliance to vCloud using vCloud Director, vCloud might override the password that you entered during OVA deployment. To prevent the override, take the following steps.
 - a After deploying in vCloud Director, click your vApp to view the vRealize Automation appliance.
 - b Right-click the vRealize Automation appliance, and select **Properties**.
 - c Click the **Guest OS Customization** tab.
 - d Under **Password Reset**, clear the **Allow local administrator password** option, and click **OK**.

- e Power on the vRealize Automation appliance.
 - f Wait for the machine to start, which might take up to 5 minutes.
- 13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Automation appliance.

Using the Installation Wizard for Minimal Deployments

Minimal deployments demonstrate how vRealize Automation works but usually do not have enough capacity to support enterprise production environments.

Install a minimal deployment for proof-of-concept work or to become familiar with vRealize Automation.

Run the Installation Wizard for a Minimal Deployment

Minimal deployments typically consist of one vRealize Automation appliance, one IaaS Windows server, and the vSphere agent for endpoints. Minimal installation places all IaaS components on a single Windows server.

Minimal deployments typically consist of one vRealize Automation appliance, one IaaS Windows server, and the vSphere agent for endpoints.

Prerequisites

- Verify that you have met the prerequisites described in [Chapter 2, “Preparing for vRealize Automation Installation,”](#) on page 19.
- [“Deploy the vRealize Automation Appliance,”](#) on page 66.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 3 When the Installation Wizard appears, click **Next**.
- 4 Accept the End User License Agreement and click **Next**.
- 5 On the Deployment Type page, select **Minimal deployment** and **Install Infrastructure as a Service**, and click **Next**.
- 6 On the Installation Prerequisites page, you pause to log in to your IaaS Windows server and install the Management Agent. The Management Agent allows the vRealize Automation appliance to discover and connect to the IaaS server.

What to do next

See [“Installing the Management Agent,”](#) on page 35.

Installing the Management Agent

You must install a Management Agent on each Windows machine hosting IaaS components.

For enterprise installations, a Management Agent is not required for the MS SQL host.

If your primary vRealize Automation appliance fails, you must reinstall Management Agents.

Management Agents are not automatically deleted when you uninstall an IaaS component. Uninstall the Management Agent as you would uninstall any Windows program with the Add or Remove program tool.

Procedure

- 1 [Find the SSL Certificate Fingerprint for the Management Site Service](#) on page 36
When you install a management agent, you must validate the fingerprint of the SSL certificate for the Management Site service.
- 2 [Download and Install the Management Agent](#) on page 36
You install the Management Agent on the IaaS Windows server in your deployment.

Find the SSL Certificate Fingerprint for the Management Site Service

When you install a management agent, you must validate the fingerprint of the SSL certificate for the Management Site service.

You can obtain the fingerprint at the command prompt on the vRealize Automation appliance.

Procedure

- 1 Log in to the vRealize Automation appliance console as root.
- 2 Enter the following command:

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


The SHA1 fingerprint appears. For example:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copy the fingerprint UID. For validation, you might need to remove the colons.

What to do next

Keep the fingerprint you copied for use with the Management Agent installer.

Download and Install the Management Agent

You install the Management Agent on the IaaS Windows server in your deployment.

The Management Agent registers the IaaS Windows server with the vRealize Automation appliance, automates the installation and management of IaaS components, and collects support and telemetry information. The Management Agent runs as a Windows service.

If you host the vRealize Automation SQL Server database on a separate Windows machine that does not host the IaaS components, the SQL Server machine does not need the Management Agent.

Prerequisites

- Note the vRealize Automation appliance certificate fingerprint by following the steps in [“Find the SSL Certificate Fingerprint for the Management Site Service,”](#) on page 36.
- Note the user name and password of a domain account with administrator privileges on the IaaS Windows server. The Management Agent service must run under this account.

Procedure

- 1 Log in to the IaaS Windows server using an account that has administrator rights.
- 2 Open a Web browser to the vRealize Automation appliance installer URL.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Click **Management Agent installer**, and save `vCAC-IaaSManagementAgent-Setup.msi`.
- 4 Run `vCAC-IaaSManagementAgent-Setup.msi`.
- 5 Read the welcome and click **Next**.

- 6 Accept the EULA and click **Next**.
- 7 Confirm or change the installation folder, and click **Next**.

The default folder is `%Program Files(x86)%\VMware\vCAC\Management Agent`.

- 8 Enter Management Site Service details.

Text box	Input
vRA appliance address	https://vrealize-automation-appliance-FQDN:5480 You must include the port number.
Root username	The root user name for the vRealize Automation appliance.
Password	The root user password for the vRealize Automation appliance.
Management Site server certificate	The SHA1 fingerprint for the Management Site Service certificate. The Management Site Service is hosted on the vRealize Automation appliance. Sample SHA1 fingerprint: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78
Load	Click Load to load the default fingerprint.

The screenshot shows the 'Management Site Service' configuration window. The title bar reads 'VMware vRealize Automation Management Agent Setup'. The main heading is 'Management Site Service' with the instruction: 'Specify the VA host for the Management Site Service to use for the agent.' Below this, there are several input fields:

- 'vRA appliance address:' with a text box containing 'https://vra-address:5480/'. A note below says: 'Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...'.
- 'Root username:' with a text box containing 'root'.
- 'Password:' with a masked text box containing ten dots.
- 'Management Site Service certificate SHA1 fingerprint:' with a text box containing '4F03BF5B12D49E351B2F6C779B2B1C2A4D10E882' and a 'Load' button to its right.

 At the bottom, there is a checked checkbox: 'I confirm the fingerprint matches the Management Site Service SSL certificate'. At the very bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.

- 9 Verify that the fingerprint matches the one from the vRealize Automation appliance certificate, and select the confirmation checkbox.

If the fingerprints do not match, verify that the correct address appears in **vRA appliance address**. Make changes and reload the fingerprint, if necessary.

- 10 Click **Next**.
- 11 Enter the service account user name and password, and click **Next**.
- 12 Click **Install**.
- 13 Click **Finish**.

After you install the Management Agent, the IaaS Windows server appears on the Installation Prerequisites page of the Installation Wizard.

Synchronize Server Times

Clocks on vRealize Automation servers and Windows servers must be synchronized to ensure a successful installation.

Options on the Prerequisites page of the Installation Wizard let you select a time synchronization method for your virtual appliances. The IaaS host table informs you of time offsets.

Procedure

- 1 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select Use Time Server from the Time Sync Mode menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the Time Server text box.
Use Host Time	Select Use Host Time from the Time Sync Mode menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

- 2 Click **Change Time Settings**.
- 3 Click **Next**.

What to do next

Verify that your IaaS servers are configured correctly.

Run the Prerequisite Checker

Run the Prerequisite Checker to verify that the Windows server for IaaS components is correctly configured.

Procedure

- 1 Click **Run** on the Prerequisite Checker screen.
As the checks are done, the Windows server for IaaS components is listed with a status.
- 2 If you see a warning, you can get more information on the error or choose to automatically correct the error.
 - ◆ Click **Show Details** for more information on the error and the course of action to follow to address it.
 - ◆ Click **Fix** to automatically fix the error.
The **Fix** option applies corrections and restarts the IaaS Windows server.
- 3 Click **Run** to verify corrections.
- 4 Click **Next** when all errors are resolved.

Your Windows server is correctly configured for installation of IaaS components.

What to do next

Continue to the vRealize Automation Host screen.

Specify Minimal Deployment Parameters

Use the vRealize Automation Installation Wizard to enter configuration settings for the minimal deployment components.

Procedure

- ◆ Follow the Installation Wizard pages to enter vRealize Automation appliance and IaaS Windows server FQDNs, account credentials, default tenant password, and other settings.

The wizard checks systems for prerequisites before you begin to enter settings, and validates your settings before it begins product installation.

What to do next

In vSphere, create a snapshot of each vRealize Automation appliance and IaaS Windows server before you begin product installation.

Create Snapshots Before You Begin the Installation

Take snapshots of all your appliances and Windows servers. If the installation fails, you can revert to these snapshots and try to install again.

The snapshots preserve your configuration work. Be sure to include a snapshot of the vRealize Automation appliance on which you are running the wizard.

Instructions are provided for vSphere users.

NOTE Do not exit the installation wizard or cancel the installation.

Procedure

- 1 Open another browser and log in to the vSphere Client.
- 2 Locate your server or appliance in the vSphere Client inventory.
- 3 Right-click the server the inventory and select **Take Snapshot**.
- 4 Enter a snapshot name.
- 5 Select **Snapshot the virtual machine's memory** checkbox to capture the memory of the server and click **OK**.

The snapshot is created.

Repeat these steps to take snapshots of each of your servers or appliances.

What to do next

[“Finish the Installation,”](#) on page 60

Finish the Installation

There are a couple final settings to apply before initiating the vRealize Automation installation and waiting for the process to complete.

Procedure

- 1 Return to the installation wizard.
- 2 Review the installation summary and click **Next**.
- 3 Enter the product license key and click **Next**.

- 4 Accept or change the default telemetry settings and click **Next**.
- 5 Click **Next**.
- 6 Click **Finish**.

The installation starts. Depending on your network, installation might take up to an hour to finish.

What to do next

Set up vRealize Automation for initial content creation.

Address Installation Failures

When you install from the Installation Details page, you are informed of any issues that are preventing the installation from finishing.

When problems are found, the component is flagged and you are presented with detailed information about the failure along with steps to investigate solutions. After you have addressed the issue, you retry the installation step. Depending on the type of failure, you follow different remediation steps.

Procedure

- 1 If the **Retry Failed** button is enabled, use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed and make required changes.
 - c Return to the Installation screen and click **Retry Failed**.
The installer attempts to install all failed components.
- 2 If the **Retry All IaaS** button is enabled, use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed.
 - c Revert all IaaS servers to the snapshots you created earlier.
 - d Delete the MS SQL database, if you are using an external database.
 - e Make required changes.
 - f Click **Retry All IaaS**.
- 3 If the failure is in the virtual appliance components use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed.
 - c Revert all servers to snapshots, including the one from which you are running the wizard,
 - d Make required changes.
 - e Refresh the wizard page.
 - f Logon and rerun the wizard again.
The wizard opens at the pre-installation step.

Set Up Credentials for Initial Content Configuration

Optionally, you can start an initial content workflow for a vSphere endpoint.

The process uses a local user called configurationadmin that is granted administrator rights.

Procedure

- 1 Create and enter a password for the configurationadmin account in the **Password** text box.
- 2 Reenter the password in the **Confirm password** text box. Make a note of the password for later use.
- 3 Click **Create Initial Content**.
- 4 Click **Next**.

A configuration admin user is created and a configuration catalog item is created in the default tenant. The configuration admin is granted the following rights:

- Approval Administrator
- Catalog Administrator
- IaaS Administrator
- Infrastructure Architect
- Tenant Administrator
- XaaS Architect

What to do next

- When you finish the wizard, you can log in to the default tenant as the configurationadmin user and request the initial content catalog items. For an example of how to request the item and complete the manual user action, see *Installing and Configuring vRealize Automation for the Rainpole Scenario*.
- Configure access to the default tenant for other users. See [“Configure Access to the Default Tenant,”](#) on page 124.

Using the Installation Wizard for Enterprise Deployments

You can tailor your enterprise deployment to the needs of your organization. An enterprise deployment can consist of distributed components or high-availability deployments configured with load balancers.

Enterprise deployments are designed for more complex installation structures with distributed and redundant components and generally include load balancers. Installation of IaaS components is optional with either type of deployment.

For load-balanced deployments, multiple active Web server instances and vRealize Automation appliance appliances cause the installation to fail. Only a single Web server instance and a single vRealize Automation appliance should be active during the installation.

Run the Installation Wizard for an Enterprise Deployment

Enterprise deployments are used for production environment. You can use the Installation Wizard to deploy a distributed installation or a distributed installation with load balancers for high availability and failover.

If you install a distributed installation with load balancers for high availability and failover, notify the team responsible for configuring your vRealize Automation environment. Your tenant administrators must configure Directories Management for high availability when they configure the link to your Active Directory.

Prerequisites

- Verify that you have met the prerequisites described in [Chapter 2, “Preparing for vRealize Automation Installation,”](#) on page 19.
- [“Deploy the vRealize Automation Appliance,”](#) on page 66.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 3 When the Installation Wizard appears, click **Next**.
- 4 Accept the End User License Agreement and click **Next**.
- 5 On the Deployment Type page, select **Enterprise deployment** and **Install Infrastructure as a Service**.
- 6 On the Installation Prerequisites page, you pause to log in to your IaaS Windows servers and install the Management Agent. The Management Agent allows the vRealize Automation appliance to discover and connect to those IaaS servers.

What to do next

See [“Installing the Management Agent,”](#) on page 42.

Installing the Management Agent

You must install a Management Agent on each Windows machine hosting IaaS components.

If your primary vRealize Automation appliance fails, you must reinstall Management Agents.

Management Agents are not automatically deleted when you uninstall an IaaS component. Uninstall the Management Agent as you would uninstall any Windows program with the Add or Remove program tool.

Find the SSL Certificate Fingerprint for the Management Site Service

When you install a management agent, you must validate the fingerprint of the SSL certificate for the Management Site service.

You can obtain the fingerprint at the command prompt on the vRealize Automation appliance.

Procedure

- 1 Log in to the vRealize Automation appliance console as root.
- 2 Enter the following command:

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


The SHA1 fingerprint appears. For example:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copy the fingerprint UID. For validation, you might need to remove the colons.

What to do next

Keep the fingerprint you copied for use with the Management Agent installer.

Download and Install the Management Agent

You install the Management Agent on each IaaS Windows server in your deployment.

The Management Agent registers the IaaS Windows server with the vRealize Automation appliance, automates the installation and management of IaaS components, and collects support and telemetry information. The Management Agent runs as a Windows service.

If you host the vRealize Automation SQL Server database on a separate Windows machine that does not host any other IaaS components, the SQL Server machine does not need the Management Agent.

Prerequisites

- Note the vRealize Automation appliance certificate fingerprint by following the steps in [“Find the SSL Certificate Fingerprint for the Management Site Service,”](#) on page 36.
- Note the user name and password of a domain account with administrator privileges on the IaaS Windows server. The Management Agent service must run under this account.

Procedure

- 1 Log in to the IaaS Windows server using an account that has administrator rights.
- 2 Open a Web browser directly to the vRealize Automation appliance installer URL. Do not use a load balancer address.

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

- 3 Click **Management Agent installer**, and save `vCAC-IaaSManagementAgent-Setup.msi`.
- 4 Run `vCAC-IaaSManagementAgent-Setup.msi`.
- 5 Read the welcome and click **Next**.
- 6 Accept the EULA and click **Next**.
- 7 Confirm or change the installation folder, and click **Next**.

The default folder is `%Program Files(x86)%\VMware\vCAC\Management Agent`.

- 8 Enter Management Site Service details.

Text box	Input
vRA appliance address	<code>https://vrealize-automation-appliance-FQDN:5480</code> You must include the port number.
Root username	The root user name for the vRealize Automation appliance.
Password	The root user password for the vRealize Automation appliance.

Text box	Input
Management Site server certificate	The SHA1 fingerprint for the Management Site Service certificate. The Management Site Service is hosted on the vRealize Automation appliance. Sample SHA1 fingerprint: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78
Load	Click Load to load the default fingerprint.

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

- Verify that the fingerprint matches the one from the vRealize Automation appliance certificate, and select the confirmation checkbox.

If the fingerprints do not match, verify that the correct address appears in **vRA appliance address**. Make changes and reload the fingerprint, if necessary.

- Click **Next**.
- Enter the service account user name and password, and click **Next**.
- Click **Install**.
- Click **Finish**.
- Repeat the process for each IaaS Windows server.

After you install the Management Agent, the IaaS Windows server appears on the Installation Prerequisites page of the Installation Wizard.

Synchronize Server Times

Clocks on vRealize Automation servers and Windows servers must be synchronized to ensure a successful installation.

Options on the Prerequisites page of the Installation Wizard let you select a time synchronization method for your virtual appliances. The IaaS host table informs you of time offsets.

Procedure

- 1 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select Use Time Server from the Time Sync Mode menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the Time Server text box.
Use Host Time	Select Use Host Time from the Time Sync Mode menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

- 2 Click **Change Time Settings**.
- 3 Click **Next**.

What to do next

Verify that your IaaS servers are configured correctly.

Run the Prerequisite Checker

Run the Prerequisite Checker to verify that the Windows servers for IaaS components are correctly configured.

Procedure

- 1 Click **Run** on the Prerequisite Checker screen.

As the checks are done, each Windows server for IaaS components is listed with a status.

- 2 If you see a warning, you can get more information on the error or choose to automatically correct the error.
 - ◆ Click **Show Details** for more information on the error and the course of action to follow to address it.
 - ◆ Click **Fix** to automatically fix the error.

The **Fix** option applies corrections and restarts all IaaS machines, including those that might not have had fixes.
- 3 Click **Run** to verify corrections.
- 4 Click **Next** when all errors are resolved.

Your Windows servers are correctly configured for installation of IaaS components.

What to do next

Continue to the vRealize Automation Host screen.

Specify Enterprise Deployment Parameters

Use the vRealize Automation Installation Wizard to enter configuration settings for the enterprise deployment components.

Prerequisites

Procedure

- ◆ Follow the Installation Wizard pages to enter vRealize Automation appliance and IaaS Windows server FQDNs, account credentials, default tenant password, and other settings.

The wizard checks systems for prerequisites before you begin to enter settings, and validates your settings before it begins product installation.

What to do next

In vSphere, create a snapshot of each vRealize Automation appliance and IaaS Windows server before you begin product installation.

Create Snapshots Before You Begin the Installation

Take snapshots of all your appliances and Windows servers. If the installation fails, you can revert to these snapshots and try to install again.

The snapshots preserve your configuration work. Be sure to include a snapshot of the vRealize Automation appliance on which you are running the wizard.

Instructions are provided for vSphere users.

NOTE Do not exit the installation wizard or cancel the installation.

Procedure

- 1 Open another browser and log in to the vSphere Client.
- 2 Locate your server or appliance in the vSphere Client inventory.
- 3 Right-click the server the inventory and select **Take Snapshot**.
- 4 Enter a snapshot name.
- 5 Select **Snapshot the virtual machine's memory** checkbox to capture the memory of the server and click **OK**.

The snapshot is created.

Repeat these steps to take snapshots of each of your servers or appliances.

What to do next

[“Finish the Installation,”](#) on page 60

Finish the Installation

After creating snapshots, you initiate the installation of vRealize Automation and wait for the installation to complete successfully.

Procedure

- 1 Return to the installation wizard.
- 2 Review the installation summary and click **Next**.

- 3 Click **Next**.
- 4 Click **Finish**.

The installation starts. Depending on your network configuration, installation can take between fifteen minutes and one hour.

A confirmation message appears when the installation finishes.

What to do next

You are now ready to configure your deployment.

Address Installation Failures

When you install from the Installation Details page, you are informed of any issues that are preventing the installation from finishing.

When problems are found, the component is flagged and you are presented with detailed information about the failure along with steps to investigate solutions. After you have addressed the issue, you retry the installation step. Depending on the type of failure, you follow different remediation steps.

Procedure

- 1 If the **Retry Failed** button is enabled, use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed and make required changes.
 - c Return to the Installation screen and click **Retry Failed**.
The installer attempts to install all failed components.
- 2 If the **Retry All IaaS** button is enabled, use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed.
 - c Revert all IaaS servers to the snapshots you created earlier.
 - d Delete the MS SQL database, if you are using an external database.
 - e Make required changes.
 - f Click **Retry All IaaS**.
- 3 If the failure is in the virtual appliance components use the following steps.
 - a Review the failure.
 - b Assess what needs to be changed.
 - c Revert all servers to snapshots, including the one from which you are running the wizard,
 - d Make required changes.
 - e Refresh the wizard page.
 - f Logon and rerun the wizard again.
The wizard opens at the pre-installation step.

Set Up Credentials for Initial Content Configuration

Optionally, you can start an initial content workflow for a vSphere endpoint.

The process uses a local user called configurationadmin that is granted administrator rights.

Procedure

- 1 Create and enter a password for the configurationadmin account in the **Password** text box.
- 2 Reenter the password in the **Confirm password** text box. Make a note of the password for later use.
- 3 Click **Create Initial Content**.
- 4 Click **Next**.

A configuration admin user is created and a configuration catalog item is created in the default tenant. The configuration admin is granted the following rights:

- Approval Administrator
- Catalog Administrator
- IaaS Administrator
- Infrastructure Architect
- Tenant Administrator
- XaaS Architect

What to do next

- When you finish the wizard, you can log in to the default tenant as the configurationadmin user and request the initial content catalog items. For an example of how to request the item and complete the manual user action, see *Installing and Configuring vRealize Automation for the Rainpole Scenario*.
- Configure access to the default tenant for other users. See [“Configure Access to the Default Tenant,”](#) on page 124.

The Standard vRealize Automation Installation Interfaces

4

After running the Installation Wizard, you might need or want to perform certain installation tasks manually, through the standard interfaces.

The Installation Wizard described in [Chapter 3, “Installing vRealize Automation with the Installation Wizard,”](#) on page 33 is your primary tool for new vRealize Automation installations. However, after you run the wizard, some operations still require the older, manual installation process.

You need the manual steps if you want to expand a vRealize Automation deployment or if the wizard stopped for any reason. Situations when you might need to refer to the procedures in this section include the following examples.

- You chose to cancel the wizard before finishing the installation.
- Installation through the wizard failed for some reason.
- You want to add another vRealize Automation appliance for high availability.
- You want to add another IaaS Web server for high availability.
- You need another proxy agent.
- You need another DEM worker or orchestrator.

You might use all or only some of the manual processes. Review the material throughout this section, and follow the procedures that apply to your situation.

This chapter includes the following topics:

- [“Using the Standard Interfaces for Minimal Deployments,”](#) on page 49
- [“Using the Standard Interfaces for Distributed Deployments,”](#) on page 60
- [“Installing vRealize Automation Agents,”](#) on page 97

Using the Standard Interfaces for Minimal Deployments

You can install a standalone, minimal deployment for use in a development environment or as a proof of concept. Minimal deployments are not suitable for a production environment.

Minimal Deployment Checklist

A system administrator can deploy a complete vRealize Automation in a minimal configuration. Minimal deployments are typically used in a development environment or as a proof of concept and require fewer steps to install.

The Minimal Deployment Checklist provides a high-level overview of the sequence of tasks you must perform to complete a minimal installation.

Print out a copy of the checklist and use it to track your work as you complete the installation. Complete the tasks in the order in which they are given.

Table 4-1. Minimal Deployment Checklist

Task	Details
<input type="checkbox"/> Plan and prepare the installation environment and verify that all installation prerequisites are met.	Chapter 2, “Preparing for vRealize Automation Installation,” on page 19
<input type="checkbox"/> Set up your vRealize Automation appliance	“Deploy and Configure the vRealize Automation Appliance,” on page 50
<input type="checkbox"/> Install IaaS components on a single Windows server.	“Installing IaaS Components,” on page 55
<input type="checkbox"/> Install additional agents, if required.	“Installing vRealize Automation Agents,” on page 97
<input type="checkbox"/> Perform post-installation tasks such as configuring the default tenant.	

Deploy and Configure the vRealize Automation Appliance

The vRealize Automation appliance is a preconfigured virtual appliance that deploys the vRealize Automation appliance server and Web console (the user portal). It is delivered as an open virtualization format (OVF) template. The system administrator downloads the appliance and deploys it into the vCenter Server or ESX/ESXi inventory.

- 1 [Deploy the vRealize Automation Appliance](#) on page 50
To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.
- 2 [Enable Time Synchronization on the vRealize Automation Appliance](#) on page 52
Clocks on the vRealize Automation server and Windows servers must be synchronized to ensure a successful installation.
- 3 [Configure the vRealize Automation Appliance](#) on page 52
To prepare the vRealize Automation appliance for use, you configure host settings, generate an SSL certificate, and provide SSO connection information.

Deploy the vRealize Automation Appliance

To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.

Some restrictions apply to the root password you create for the vRealize Automation administrator.

Prerequisites

- Download the vRealize Automation appliance from the VMware Web site.
- Log in to the vSphere client as a user with system administrator privileges.

Procedure

- 1 Select **File > Deploy OVF Template** from the vSphere client.
- 2 Browse to the vRealize Automation appliance file you downloaded and click **Open**.
- 3 Click **Next**.
- 4 Click **Next** on the OVF Template Details page.
- 5 Accept the license agreement and click **Next**.

- 6 Enter a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.
- 7 Follow the prompts until the Disk Format page appears.
- 8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.
- 9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

- 10 Configure the values on the Properties page.
 - a Enter the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.
 - b Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

This value is used to set the initial status of the SSH service in the appliance. If you are installing with the Installation Wizard, enable this before you begin the wizard. You can change this setting from the appliance management console after installation.
 - c Enter the fully qualified domain name of the virtual machine in the **Hostname** text box.
 - d Configure the networking properties.
- 11 Click **Next**.
- 12 Depending on your deployment, vCenter, and DNS configuration, select one of the following ways of finishing OVA deployment and powering up the vRealize Automation appliance.
 - If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.
 - a Select **Power on after deployment** and click **Finish**.
 - b After the file finishes deploying into vCenter, click **Close**.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
 - a After the file finishes deploying into vCenter, click **Close**.
 - b Power on the vRealize Automation appliance.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - d Verify that you can ping the DNS for the vRealize Automation appliance. If you cannot ping the DNS, restart the virtual machine.
 - e Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed the vRealize Automation appliance to vCloud using vCloud Director, vCloud might override the password that you entered during OVA deployment. To prevent the override, take the following steps.
 - a After deploying in vCloud Director, click your vApp to view the vRealize Automation appliance.
 - b Right-click the vRealize Automation appliance, and select **Properties**.
 - c Click the **Guest OS Customization** tab.
 - d Under **Password Reset**, clear the **Allow local administrator password** option, and click **OK**.

- e Power on the vRealize Automation appliance.
 - f Wait for the machine to start, which might take up to 5 minutes.
- 13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Automation appliance.

Enable Time Synchronization on the vRealize Automation Appliance

Clocks on the vRealize Automation server and Windows servers must be synchronized to ensure a successful installation.

If you see certificate warnings during this process, continue past them to finish the installation.

Prerequisites

[“Deploy the vRealize Automation Appliance,”](#) on page 33.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
- 2 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 3 Select **Admin > Time Settings**.
- 4 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select Use Time Server from the Time Sync Mode menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the Time Server text box.
Use Host Time	Select Use Host Time from the Time Sync Mode menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

- 5 Click **Save Settings**.
- 6 Click **Refresh**.
- 7 Verify that the value in **Current Time** is correct.
You can change the time zone as required from the Time Zone Setting page on the **System** tab.
- 8 (Optional) Click **Time Zone** from the **System** tab and select a system time zone from the menu choices.
The default is Etc/UTC.
- 9 Click **Save Settings**.

Configure the vRealize Automation Appliance

To prepare the vRealize Automation appliance for use, you configure host settings, generate an SSL certificate, and provide SSO connection information.

Prerequisites

[“Enable Time Synchronization on the vRealize Automation Appliance,”](#) on page 52.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
`https://vrealize-automation-appliance-FQDN:5480`

- 2 Continue past the certificate warning.
- 3 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 4 Select **vRA Settings > Host Settings**.

Option	Action
Resolve Automatically	Select Resolve Automatically to specify the name of the current host for the vRealize Automation appliance.
Update Host	<p>For new hosts, select Update Host. Enter the fully qualified domain name of the vRealize Automation appliance, <i>vra-hostname.domain.name</i>, in the Host Name text box.</p> <p>For distributed deployments that use load balancers, select Update Host. Enter the fully qualified domain name for the load balancer server, <i>vra-loadbalancename.domain.name</i>, in the Host Name text box.</p>

NOTE Configure SSO settings as described later in this procedure whenever you use **Update Host** to set the host name.

- 5 Select the certificate type from the **Certificate Action** menu.

If you are using a PEM-encoded certificate, for example for a distributed environment, select **Import**.

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Automation appliance and any load balancer through the use of Subject Alternative Name (SAN) certificates.

NOTE If you use certificate chains, specify the certificates in the following order:

- a Client/server certificate signed by the intermediate CA certificate
 - b One or more intermediate certificates
 - c A root CA certificate
-

Option	Action
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.
Generate Certificate	<ol style="list-style-type: none"> a The value displayed in the Common Name text box is the Host Name as it appears on the upper part of the page. If any additional instances of the vRealize Automation appliance available, their FQDNs are included in the SAN attribute of the certificate. b Enter your organization name, such as your company name, in the Organization text box. c Enter your organizational unit, such as your department name or location, in the Organizational Unit text box. d Enter a two-letter ISO 3166 country code, such as US, in the Country text box.
Import	<ol style="list-style-type: none"> a Copy the certificate values from BEGIN PRIVATE KEY to END PRIVATE KEY, including the header and footer, and paste them in the RSA Private Key text box. b Copy the certificate values from BEGIN CERTIFICATE to END CERTIFICATE, including the header and footer, and paste them in the Certificate Chain text box. For multiple certificate values, include a BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate. NOTE In the case of chained certificates, additional attributes may be available. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the Passphrase text box.

- 6 Click **Save Settings** to save host information and SSL configuration.
- 7 Configure the SSO settings.
- 8 Click **Messaging**. The configuration settings and status of messaging for your appliance is displayed. Do not change these settings.
- 9 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

- Select **Join the VMware Customer Experience Improvement Program** to participate in the program.
- Deselect **Join the VMware Customer Experience Improvement Program** to not participate in the program.

- 10 Click **Services** and verify that services are registered.

Depending on your site configuration, this can take about 10 minutes.

NOTE You can log in to the appliance and run `tail -f /var/log/vcac/catalina.out` to monitor startup of the services.

- 11 Enter your license information.
 - a Click **vRA Settings > Licensing**.
 - b Click **Licensing**.
 - c Enter a valid vRealize Automation license key that you downloaded when you downloaded the installation files, and click **Submit Key**.

NOTE If you experience a connection error, you might have a problem with the load balancer. Check network connectivity to the load balancer.

- 12 Confirm that you can log in to vRealize Automation.
 - a Open a Web browser to the vRealize Automation product interface URL.
`https://vrealize-automation-appliance-FQDN/vcac`
 - b Accept the vRealize Automation certificate.
 - c Accept the SSO certificate.
 - d Log in with `administrator@vsphere.local` and the password you specified when you configured SSO.

The interface opens to the Tenants page on the **Administration** tab. A single tenant named `vsphere.local` appears in the list.

You have finished the deployment and configuration of your vRealize Automation appliance. If the appliance does not function correctly after configuration, redeploy and reconfigure the appliance. Do not make changes to the existing appliance.

What to do next

See [“Install the Infrastructure Components,”](#) on page 56.

Installing IaaS Components

The administrator installs a complete set of infrastructure (IaaS) components on a Windows machine (physical or virtual). Administrator rights are required to perform these tasks.

A minimal installation installs all of the components on the same Windows server, except for the SQL database, which you can install on a separate server.

Enable Time Synchronization on the Windows Server

Clocks on the vRealize Automation server and Windows servers must be synchronized to ensure that the installation is successful.

The following steps describe how to enable time synchronization with the ESX/ESXi host by using VMware Tools. If you are installing the IaaS components on a physical host or do not want to use VMware Tools for time synchronization, ensure that the server time is accurate by using your preferred method.

Procedure

- 1 Open a command prompt on the Windows installation machine.

- 2 Type the following command to navigate to the VMware Tools directory.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 Type the command to display the timesync status.

```
VMwareToolboxCmd.exe timesync status
```

- 4 If timesync is disabled, type the following command to enable it.

```
VMwareToolboxCmd.exe timesync enable
```

IaaS Certificates

vRealize Automation IaaS components use certificates and SSL to secure communications between components. In a minimal installation for proof-of-concept purposes, you can use self-signed certificates.

In a distributed environment, obtain a domain certificate from a trusted certificate authority. For information about installing domain certificates for IaaS components, see [“Install IaaS Certificates,”](#) on page 75 in the distributed deployment chapter.

Install the Infrastructure Components

The system administrator logs into the Windows machine and follows the installation wizard to install the infrastructure components (IaaS) on the Windows virtual or physical machine.

Prerequisites

- Verify that your installation machine meets the requirements described in [“IaaS Web Service and Model Manager Server Requirements,”](#) on page 22.
- [“Enable Time Synchronization on the Windows Server,”](#) on page 55.
- Verify that you have deployed and fully configured the vRealize Automation appliance, and that the necessary services are running (plugin-service, catalog-service, iaas-proxy-provider).

Procedure

- 1 [Download the vRealize Automation IaaS Installer](#) on page 57
To install IaaS on your minimal virtual or physical Windows server, you download a copy of the IaaS installer from the vRealize Automation appliance.
- 2 [Select the Installation Type](#) on page 57
The system administrator runs the installer wizard from the Windows 2008 or 2012 installation machine.
- 3 [Check Prerequisites](#) on page 58
The Prerequisite Checker verifies that your machine meets IaaS installation requirements.
- 4 [Specify Server and Account Settings](#) on page 58
The vRealize Automation system administrator specifies server and account settings for the Windows installation server and selects a SQL database server instance and authentication method.
- 5 [Specify Managers and Agents](#) on page 59
The minimum installation installs the required Distributed Execution Managers and the default vSphere proxy agent. The system administrator can install additional proxy agents (XenServer, or Hyper-V, for example) after installation using the custom installer.
- 6 [Register the IaaS Components](#) on page 59
The system administrator installs the IaaS certificate and registers the IaaS components with the SSO.
- 7 [Finish the Installation](#) on page 60
The system administrator finishes the IaaS installation.

Download the vRealize Automation IaaS Installer

To install IaaS on your minimal virtual or physical Windows server, you download a copy of the IaaS installer from the vRealize Automation appliance.

If you see certificate warnings during this process, continue past them to finish the installation.

Prerequisites

- Microsoft .NET Framework 4.5.2 or later. You can download the .NET installer from the same Web page as the IaaS installer.
- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. Point Internet Explorer to `res://iesetup.dll/SoftAdmin.htm` on the Windows server.

Procedure

- 1 Log in to the IaaS Windows server using an account that has administrator rights.
- 2 Open a Web browser directly to the vRealize Automation appliance installer URL.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Click **IaaS Installer**.
- 4 Save `setup__vrealize-automation-appliance-FQDN@5480` to the Windows server.
Do not change the installer file name. It is used to connect the installation to the vRealize Automation appliance.

Select the Installation Type

The system administrator runs the installer wizard from the Windows 2008 or 2012 installation machine.

Prerequisites

[“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Accept Certificate**.
- 6 Click **Next**.

- 7 Select **Complete Install** on the Installation Type page if you are creating a minimal deployment and click **Next**.

Check Prerequisites

The Prerequisite Checker verifies that your machine meets IaaS installation requirements.

Prerequisites

[“Select the Installation Type,”](#) on page 57.

Procedure

- 1 Complete the Prerequisite Check.

Option	Description
No errors	Click Next .
Noncritical errors	Click Bypass .
Critical errors	Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click Check Again to verify.

- 2 Click **Next**.

The machine meets installation requirements.

Specify Server and Account Settings

The vRealize Automation system administrator specifies server and account settings for the Windows installation server and selects a SQL database server instance and authentication method.

Prerequisites

[“Check Prerequisites,”](#) on page 58.

Procedure

- 1 On the Server and Account Settings page or the Detected Settings page, enter the user name and password for the Windows service account. This service account must be a local administrator account that also has SQL administrative privileges.

- 2 Type a phrase in the **Passphrase** text box.

The passphrase is a series of words that generates the encryption key used to secure database data.

NOTE Save your passphrase so that it is available for future installations or system recovery.

- 3 To install the database instance on the same server with the IaaS components, accept the default server in the **Server** text box in the SQL Server Database Installation Information section.

If the database is on a different machine, enter the server in the following format.

machine-FQDN,port-number\named-database-instance

- 4 Accept the default in the **Database name** text box, or enter the appropriate name if applicable.

- 5 Select the authentication method.
 - ◆ Select **Use Windows authentication** if you want to create the database using the Windows credentials of the current user. The user must have SQL sys_admin privileges.
 - ◆ Deselect **Use Windows authentication** if you want to create the database using SQL authentication. Type the **User name** and **Password** of the SQL Server user with SQL sys_admin privileges on the SQL server instance.

Windows authentication is recommended. When you choose SQL authentication, the unencrypted database password appears in certain configuration files.

- 6 (Optional) Select the **Use SSL for database connection** checkbox.

By default, the checkbox is enabled. SSL provides a more secure connection between the IaaS server and SQL database. However, you must first configure SSL on the SQL server to support this option. For more about configuring SSL on the SQL server, see [Microsoft Knowledge Base article 316898](#).

- 7 Click **Next**.

Specify Managers and Agents

The minimum installation installs the required Distributed Execution Managers and the default vSphere proxy agent. The system administrator can install additional proxy agents (XenServer, or Hyper-V, for example) after installation using the custom installer.

Prerequisites

[“Specify Server and Account Settings,”](#) on page 58.

Procedure

- 1 On the Distributed Execution Managers And Proxy vSphere Agent page, accept the defaults or change the names if appropriate.
- 2 Accept the default to install a vSphere agent to enable provisioning with vSphere or deselect it if applicable.
 - a Select **Install and configure vSphere agent**.
 - b Accept the default agent and endpoint, or type a name.

Make a note of the Endpoint name value. You must type this information correctly when you configure the vSphere endpoint in the vRealize Automation console or configuration may fail.
- 3 Click **Next**.

Register the IaaS Components

The system administrator installs the IaaS certificate and registers the IaaS components with the SSO.

Prerequisites

[“Download the vRealize Automation IaaS Installer,”](#) on page 57.

Procedure

- 1 Accept the default **Server** value, which is populated with the fully qualified domain name of the vRealize Automation appliance server from which you downloaded the installer. Verify that a fully qualified domain name is used to identify the server and not an IP address.

If you have multiple virtual appliances and are using a load balancer, enter the load balancer virtual appliance path.
- 2 Click **Load** to populate the value of **SSO Default Tenant** (vsphere.local).

- 3 Click **Download** to retrieve the certificate from the vRealize Automation appliance.
You can click **View Certificate** to view the certificate details.
- 4 Select **Accept Certificate** to install the SSO certificate.
- 5 In the SSO Administrator panel, type **administrator** in the **User name** text box and the password you defined for this user when you configured SSO in **Password** and **Confirm password**.
- 6 Click the test link to the right of the **User name** field to validate the entered password.
- 7 Accept the default in **IaaS Server**, which contains the host name of the Windows machine where you are installing.
- 8 Click the test link to the right of the **IaaS Server** field to validate connectivity.
- 9 Click **Next**.
If any errors appear after you click **Next**, resolve them before proceeding.

Finish the Installation

The system administrator finishes the IaaS installation.

Prerequisites

- [“Register the IaaS Components,”](#) on page 59.
- Verify that machine on which you are installing is connected to the network and is able to connect to the vRealize Automation appliance from which you download the IaaS installer.

Procedure

- 1 Review the information on the Ready to Install page and click **Install**.
The installation starts. Depending on your network configuration, installation can take between five minutes and one hour.
- 2 When the success message appears, leave the **Guide me through initial configuration** check box selected and click **Next**, and **Finish**.
- 3 Close the **Configure the System** message box.

The installation is now finished.

What to do next

[“Verify IaaS Services,”](#) on page 97.

Using the Standard Interfaces for Distributed Deployments

In a distributed, enterprise deployment, the system administrator installs components on multiple machines in the deployment environment.

Distributed Deployment Checklist

A system administrator can deploy vRealize Automation in a distributed configuration, which provides failover protection and high-availability through redundancy.

The Distributed Deployment Checklist provides a high-level overview of the steps required to perform a distributed installation.

Table 4-2. Distributed Deployment Checklist

Task	Details
<input type="checkbox"/> Plan and prepare the installation environment and verify that all installation prerequisites are met.	Chapter 2, “Preparing for vRealize Automation Installation,” on page 19
<input type="checkbox"/> Plan for and obtain your SSL certificates.	“Certificate Trust Requirements in a Distributed Deployment,” on page 63
<input type="checkbox"/> Deploy the lead vRealize Automation appliance server, and any additional appliances you require for redundancy and high availability.	“Deploy the vRealize Automation Appliance,” on page 66
<input type="checkbox"/> Configure your load balancer to handle vRealize Automation appliance traffic.	“Configuring Your Load Balancer,” on page 68
<input type="checkbox"/> Configure the lead vRealize Automation appliance server, and any additional appliances you deployed for redundancy and high availability.	“Configuring Appliances for vRealize Automation,” on page 68
<input type="checkbox"/> Configure your load balancer to handle the vRealize Automation IaaS component traffic and install vRealize Automation IaaS components.	“Install the IaaS Components in a Distributed Configuration,” on page 74
<input type="checkbox"/> If required, install agents to integrate with external systems.	“Installing vRealize Automation Agents,” on page 97
<input type="checkbox"/> Configure the default tenant and provide the IaaS license.	“Configure Access to the Default Tenant,” on page 124

vRealize Orchestrator

The vRealize Automation appliance includes an embedded version of vRealize Orchestrator that is now recommended for use with new installations. In older deployments or special cases, however, users might connect vRealize Automation to a separate, external vRealize Orchestrator. See <https://www.vmware.com/products/vrealize-orchestrator.html>.

For information about connecting vRealize Automation and vRealize Orchestrator, see *Using the vRealize Orchestrator Plug-In for vRealize Automation*.

Directories Management

If you install a distributed installation with load balancers for high availability and failover, notify the team responsible for configuring your vRealize Automation environment. Your tenant administrators must configure Directories Management for high availability when they configure the link to your Active Directory.

For more information about configuring Directories Management for high availability, see the *Configuring vRealize Automation* guide.

Distributed Installation Components

In a distributed installation, the system administrator deploys virtual appliances and related components to support the deployment environment.

Table 4-3. Virtual Appliances and Appliance Database

Component	Description
vRealize Automation appliance	A preconfigured virtual appliance that deploys the vRealize Automation server. The server includes the vRealize Automation console, which provides a single portal for self-service provisioning and management of cloud services, as well as authoring and administration.
Appliance Database	Stores information required by the virtual appliances. The database is embedded on one or two instances of vRealize Automation appliance.

You can select the individual IaaS components you want to install and specify the installation location.

Table 4-4. IaaS Components

Component	Description
Website	Provides the infrastructure administration and service authoring capabilities to the vRealize Automation console. The Website component communicates with the Model Manager, which provides it with updates from the Distributed Execution Manager (DEM), proxy agents and database.
Manager Service	The Manager Service coordinates communication between agents, the database, Active Directory, and SMTP. The Manager Service communicates with the console Web site through the Model Manager. This service requires administrative privileges to run.
Model Manager	The Model Manager communicates with the database, the DEMs, and the portal website. The Model Manager is divided into two separately installable components — the Model Manager Web service and the Model Manager data component.
Distributed Execution Managers (Orchestrator and Worker)	A Distributed Execution Manager (DEM) executes the business logic of custom models, interacting with the IaaS database and external databases. DEMs also manage cloud and physical machines.
Agents	Virtualization, integration, and WMI agents that communicate with infrastructure resources.

Disabling Load Balancer Health Checks

Health checks ensure that a load balancer sends traffic only to nodes that are working. The load balancer sends a health check at a specified frequency to every node. Nodes that exceed the failure threshold become ineligible for new traffic.

For workload distribution and failover, you may place multiple vRealize Automation appliances behind a load balancer. In addition, you may place multiple IaaS Web servers and multiple IaaS Manager Service servers behind their respective load balancers.

When using load balancers, do not allow the load balancers to send health checks at any time during installation. Health checks might interfere with installation or cause the installation to behave unpredictably.

- When deploying vRealize Automation appliance or IaaS components behind existing load balancers, disable health checks on all load balancers in the proposed configuration before installing any components.
- After installing and configuring all of vRealize Automation, including all vRealize Automation appliance and IaaS components, you may re-enable health checks.

Certificate Trust Requirements in a Distributed Deployment

For secure communication, vRealize Automation relies on certificates to create trusted relationships among components.

The specific implementation of the certificates required to achieve this trust depends on your environment.

To provide high availability and failover support, you might deploy load-balanced clusters of components. In this case, you obtain a multiple-use certificate that includes the IaaS component in the cluster, and then copy that multiple-use certificate to each component. You can use Subject Alternative Name (SAN) certificates, wildcard certificates, or any other method of multiple-use certification appropriate for your environment as long as you satisfy the trust requirements. If you use load balancers in your deployment, you must include the load balancer FQDN in the trusted address of the cluster multiple-use certificate.

For example, if you have a load balancer on the Web components cluster, one that requires a certificate on the load balancer as well as the Web components behind it, you might obtain a SAN certificate to certify `web-load-balancer.mycompany.com`, `web1.mycompany.com`, and `web2.mycompany.com`. You would copy that single multiple-use certificate to the load balancer and vRealize Automation appliances, and then register the certificate on the two Web component machines.

The Certificate Trust Requirements table summarizes the trust registration requirements for various imported certificates.

Table 4-5. Certificate Trust Requirements

Import	Register
vRealize Automation appliance cluster	Web components cluster
Web component cluster	<ul style="list-style-type: none"> ■ vRealize Automation appliance cluster ■ Manager Service components cluster ■ DEM Orchestrators and DEM Worker components
Manager Service component cluster	<ul style="list-style-type: none"> ■ DEM Orchestrators and DEM Worker components ■ Agents and Proxy Agents

Configure Web Component, Manager Service and DEM Host Certificate Trust

Customers who use a thumb print with pre installed PFX files to support user authentication must configure thumb print trust on the web host, manager service, and DEM Orchestrator and Worker host machines.

Customers who import PEM files or use self-signed certificates can ignore this procedure.

Prerequisites

Valid `web.pfx` and `ms.pfx` available for thumb print authentication.

Procedure

- 1 Import the `web.pfx` and `ms.pfx` files to the following locations on the web component and manager service host machines:
 - `Host Computer/Certificates/Personal` certificate store
 - `Host Computer/Certificates/Trusted People` certificate store
- 2 Import the `web.pfx` and `ms.pfx` files to the following locations on the DEM Orchestrator and Worker host machines:
 - `Host Computer/Certificates/Trusted People` certificate store

- 3 Open a Microsoft Management Console window on each of the applicable host machines.

NOTE Actual paths and options in the Management Console may differ somewhat based on Windows versions and system configurations.

- a Select **Add/Remove Snap-in**.
- b Select **Certificates**.
- c Select **Local Computer**.
- d Open the certificate files that you imported previously and copy the thumb prints.

What to do next

Insert the thumb print into the vRealize Automation wizard Certificate page for the Manager Service, Web components and DEM components.

Installation Worksheets

Worksheets record important information that you need to reference during installation.

Settings are case sensitive. Note that there are additional spaces for more components, if you are installing a distributed deployment. You might not need all the spaces in the worksheets. In addition, a machine might host more than one IaaS component. For example, the primary Web server and DEM Orchestrator might be on the same FQDN.

Table 4-6. vRealize Automation Appliance

Variable	My Value	Example
Primary vRealize Automation appliance FQDN		automation.mycompany.com
Primary vRealize Automation appliance IP address For reference only; do not enter IP addresses		123.234.1.105
Additional vRealize Automation appliance FQDN		automation2.mycompany.com
Additional vRealize Automation appliance IP address For reference only; do not enter IP addresses		123.234.1.106
vRealize Automation appliance load balancer FQDN		automation-balance.mycompany.com
vRealize Automation appliance load balancer IP address For reference only; do not enter IP addresses		123.234.1.201
Management interface (https://appliance-FQDN:5480) username	root (default)	root
Management interface password		admin123
Default tenant	vsphere.local (default)	vsphere.local
Default tenant username	administrator@vsphere.local (default)	administrator@vsphere.local
Default tenant password		login123

Table 4-7. IaaS Windows Servers

Variable	My Value	Example
Primary IaaS Web Server with Model Manager Data FQDN		web.mycompany.com
Primary IaaS Web Server with Model Manager Data IP address For reference only; do not enter IP addresses		123.234.1.107
Additional IaaS Web Server FQDN		web2.mycompany.com
Additional IaaS Web Server IP address For reference only; do not enter IP addresses		123.234.1.108
IaaS Web Server load balancer FQDN		web-balance.mycompany.com
IaaS Web Server load balancer IP address For reference only; do not enter IP addresses		123.234.1.202
Active IaaS Manager Service host FQDN		mgr-svc.mycompany.com
Active IaaS Manager Service host IP address For reference only; do not enter IP addresses		123.234.1.109
Passive IaaS Manager Service host FQDN		mgr-svc2.mycompany.com
Passive IaaS Manager Service host IP address For reference only; do not enter IP addresses		123.234.1.110
IaaS Manager Service host load balancer FQDN		mgr-svc-balance.mycompany.com
IaaS Manager Service host load balancer IP address For reference only; do not enter IP addresses		123.234.203
For IaaS services, domain account with administrator rights on hosts		SUPPORT\provisioner
Account password		login123

Table 4-8. IaaS SQL Server Database

Variable	My Value	Example
Database instance		IAASSQL
Database name	vcac (default)	vcac
Passphrase (used at installation, upgrade, and migration)		login123

Table 4-9. IaaS Distributed Execution Managers

Variable	My Value	Example
DEM host FQDN		dem.mycompany.com
DEM host IP address For reference only; do not enter IP addresses		123.234.1.111
DEM host FQDN		dem2.mycompany.com
DEM host IP address For reference only; do not enter IP addresses		123.234.1.112
Unique DEM Orchestrator name		Orchestrator-1
Unique DEM Orchestrator name		Orchestrator-2
Unique DEM Worker name		Worker-1
Unique DEM Worker name		Worker-2
Unique DEM Worker name		Worker-3
Unique DEM Worker name		Worker-4

Deploy the vRealize Automation Appliance

To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.

Some restrictions apply to the root password you create for the vRealize Automation administrator.

Prerequisites

- Download the vRealize Automation appliance from the VMware Web site.
- Log in to the vSphere client as a user with system administrator privileges.

Procedure

- 1 Select **File > Deploy OVF Template** from the vSphere client.
- 2 Browse to the vRealize Automation appliance file you downloaded and click **Open**.
- 3 Click **Next**.
- 4 Click **Next** on the OVF Template Details page.
- 5 Accept the license agreement and click **Next**.
- 6 Enter a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.
- 7 Follow the prompts until the Disk Format page appears.
- 8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.
- 9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

- 10 Configure the values on the Properties page.
 - a Enter the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.
 - b Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

This value is used to set the initial status of the SSH service in the appliance. If you are installing with the Installation Wizard, enable this before you begin the wizard. You can change this setting from the appliance management console after installation.
 - c Enter the fully qualified domain name of the virtual machine in the **Hostname** text box.
 - d Configure the networking properties.
- 11 Click **Next**.
- 12 Depending on your deployment, vCenter, and DNS configuration, select one of the following ways of finishing OVA deployment and powering up the vRealize Automation appliance.
 - If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.
 - a Select **Power on after deployment** and click **Finish**.
 - b After the file finishes deploying into vCenter, click **Close**.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
 - a After the file finishes deploying into vCenter, click **Close**.
 - b Power on the vRealize Automation appliance.
 - c Wait for the machine to start, which might take up to 5 minutes.
 - d Verify that you can ping the DNS for the vRealize Automation appliance. If you cannot ping the DNS, restart the virtual machine.
 - e Wait for the machine to start, which might take up to 5 minutes.
 - If you deployed the vRealize Automation appliance to vCloud using vCloud Director, vCloud might override the password that you entered during OVA deployment. To prevent the override, take the following steps.
 - a After deploying in vCloud Director, click your vApp to view the vRealize Automation appliance.
 - b Right-click the vRealize Automation appliance, and select **Properties**.
 - c Click the **Guest OS Customization** tab.
 - d Under **Password Reset**, clear the **Allow local administrator password** option, and click **OK**.
 - e Power on the vRealize Automation appliance.
 - f Wait for the machine to start, which might take up to 5 minutes.

To verify that you successfully deployed the appliance, open a command prompt and ping the FQDN of the vRealize Automation appliance.

What to do next

Repeat this procedure to deploy additional instances of the vRealize Automation appliance for redundancy in a high-availability environment.

Configuring Your Load Balancer

After you deploy the appliances for vRealize Automation, you can set up a load balancer to distribute traffic among multiple instances of the vRealize Automation appliance.

The following list provides an overview of the general steps required to configure a load balancer for vRealize Automation traffic:

- 1 Install your load balancer.
- 2 Enable session affinity, also known as sticky sessions.
- 3 Ensure that the timeout on the load balancer is at least 100 seconds.
- 4 If your network or load balancer requires it, import a certificate to your load balancer. For information about trust relationships and certificates, see [“Certificate Trust Requirements in a Distributed Deployment,”](#) on page 63. For information about extracting certificates, see [“Extracting Certificates and Private Keys,”](#) on page 30
- 5 Configure the load balancer for vRealize Automation appliance traffic.
- 6 Configure the appliances for vRealize Automation. See [“Configuring Appliances for vRealize Automation,”](#) on page 68.

NOTE When you set up virtual appliances under the load balancer, do so only for virtual appliances that have been configured for use with vRealize Automation. If unconfigured appliances are set up, you see fault responses.

For information about scalability and high availability, see the *vRealize Automation Reference Architecture* guide.

Configuring Appliances for vRealize Automation

After deploying your appliances and configuring load balancing, you configure the appliances for vRealize Automation.

Configure the Primary vRealize Automation Appliance

The vRealize Automation appliance is a preconfigured virtual appliance that deploys the vRealize Automation server and Web console (the user portal). It is delivered as an open virtualization format (OVF) template. The system administrator downloads the appliance and deploys it into the vCenter Server or ESX/ESXi inventory.

If your network or load balancer requires it, the certificate you configure for the primary instance of the appliance is copied to the load balancer and additional appliance instances in subsequent procedures.

Prerequisites

- [“Deploy the vRealize Automation Appliance,”](#) on page 66.
- Get a domain certificate for the vRealize Automation appliance.

Procedure

- 1 [Enable Time Synchronization on the vRealize Automation appliance](#) on page 69
Clocks on the vRealize Automation appliance server and Windows servers must be synchronized to ensure a successful installation.
- 2 [Configure the vRealize Automation Appliance](#) on page 69
To prepare the vRealize Automation appliance for use, you configure host settings, generate an SSL certificate, and provide SSO connection information.

Enable Time Synchronization on the vRealize Automation appliance

Clocks on the vRealize Automation appliance server and Windows servers must be synchronized to ensure a successful installation.

If you see certificate warnings during this process, continue past them to finish the installation.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
- 2 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 3 Select **Admin > Time Settings**.
- 4 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select Use Time Server from the Time Sync Mode menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the Time Server text box.
Use Host Time	Select Use Host Time from the Time Sync Mode menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

- 5 Click **Save Settings**.
- 6 Verify that the value in **Current Time** is correct.

You can change the time zone as required from the Time Zone Setting page on the **System** tab.

Configure the vRealize Automation Appliance

To prepare the vRealize Automation appliance for use, you configure host settings, generate an SSL certificate, and provide SSO connection information.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Continue past the certificate warning.
- 3 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 4 Select **vRA Settings > Host Settings**.

Option	Action
Resolve Automatically	Select Resolve Automatically to specify the name of the current host for the vRealize Automation appliance.
Update Host	For new hosts, select Update Host . Enter the fully qualified domain name of the vRealize Automation appliance, <i>vra-hostname.domain.name</i> , in the Host Name text box. For distributed deployments that use load balancers, select Update Host . Enter the fully qualified domain name for the load balancer server, <i>vra-loadbalancename.domain.name</i> , in the Host Name text box.

NOTE Configure SSO settings as described later in this procedure whenever you use **Update Host** to set the host name.

- 5 Select the certificate type from the **Certificate Action** menu.

If you are using a PEM-encoded certificate, for example for a distributed environment, select **Import**.

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Automation appliance and any load balancer through the use of Subject Alternative Name (SAN) certificates.

NOTE If you use certificate chains, specify the certificates in the following order:

- a Client/server certificate signed by the intermediate CA certificate
 - b One or more intermediate certificates
 - c A root CA certificate
-

Option	Action
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.
Generate Certificate	<ol style="list-style-type: none"> a The value displayed in the Common Name text box is the Host Name as it appears on the upper part of the page. If any additional instances of the vRealize Automation appliance available, their FQDNs are included in the SAN attribute of the certificate. b Enter your organization name, such as your company name, in the Organization text box. c Enter your organizational unit, such as your department name or location, in the Organizational Unit text box. d Enter a two-letter ISO 3166 country code, such as US, in the Country text box.
Import	<ol style="list-style-type: none"> a Copy the certificate values from BEGIN PRIVATE KEY to END PRIVATE KEY, including the header and footer, and paste them in the RSA Private Key text box. b Copy the certificate values from BEGIN CERTIFICATE to END CERTIFICATE, including the header and footer, and paste them in the Certificate Chain text box. For multiple certificate values, include a BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate. NOTE In the case of chained certificates, additional attributes may be available. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the Passphrase text box.

- 6 Click **Save Settings** to save host information and SSL configuration.
- 7 If required by your network or load balancer, copy the imported or newly created certificate to the virtual appliance load balancer.

You might need to enable root SSH access in order to export the certificate.

- a If not already logged in, log in to the vRealize Automation appliance Management Console as root.
- b Click the **Admin** tab.
- c Click the **Admin** sub menu.
- d Select the **SSH service enabled** check box.

Deselect the check box to disable SSH when finished.

- e Select the **Administrator SSH login** check box.
Deselect the check box to disable SSH when finished.
 - f Click **Save Settings**.
- 8 Configure the SSO settings.
- 9 Click **Services**.
- All services must be running before you can install a license or log in to the console. They usually start in about 10 minutes.

NOTE You can also log in to the appliance and run `tail -f /var/log/vcac/catalina.out` to monitor service startup.

- 10 Enter your license information.
- a Click **vRA Settings > Licensing**.
 - b Click **Licensing**.
 - c Enter a valid vRealize Automation license key that you downloaded when you downloaded the installation files, and click **Submit Key**.

NOTE If you experience a connection error, you might have a problem with the load balancer. Check network connectivity to the load balancer.

- 11 Click **Messaging**. The configuration settings and status of messaging for your appliance is displayed. Do not change these settings.
- 12 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).
- Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.
- Select **Join the VMware Customer Experience Improvement Program** to participate in the program.
 - Deselect **Join the VMware Customer Experience Improvement Program** to not participate in the program.
- 13 Click **Save Settings**.
- 14 Confirm that you can log in to vRealize Automation.
- a Open a Web browser to the vRealize Automation product interface URL.
`https://vrealize-automation-appliance-FQDN/vcac`
 - b If prompted, continue past the certificate warnings.
 - c Log in with `administrator@vsphere.local` and the password you specified when you configured SSO.
- The interface opens to the Tenants page on the **Administration** tab. A single tenant named `vsphere.local` appears in the list.

Configuring Additional Instances of the vRealize Automation Appliance

The system administrator can deploy multiple instances of the vRealize Automation appliance to ensure redundancy in a high-availability environment.

For each vRealize Automation appliance, you must enable time synchronization and add the appliance to a cluster. Configuration information based on settings for the initial (primary) vRealize Automation appliance is added automatically when you add the appliance to the cluster.

If you install a distributed installation with load balancers for high availability and failover, notify the team responsible for configuring your vRealize Automation environment. Your tenant administrators must configure Directories Management for high availability when they configure the link to your Active Directory.

Enable Time Synchronization on the vRealize Automation Appliance

Clocks on the vRealize Automation appliance server and Windows servers must be synchronized to ensure a successful installation.

If you see certificate warnings during this process, continue past them to finish the installation.

Prerequisites

[“Configure the Primary vRealize Automation Appliance,”](#) on page 68.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
- 2 Log in with the user name **root** and the password you specified when the appliance was deployed.
- 3 Select **Admin > Time Settings**.
- 4 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select Use Time Server from the Time Sync Mode menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the Time Server text box.
Use Host Time	Select Use Host Time from the Time Sync Mode menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

- 5 Click **Save Settings**.
- 6 Verify that the value in **Current Time** is correct.

You can change the time zone as required from the Time Zone Setting page on the **System** tab.

Add Another vRealize Automation Appliance to the Cluster

For high availability, distributed installations can use a load balancer in front of a cluster of vRealize Automation appliance nodes.

You use the management console on the new vRealize Automation appliance to join it to an existing cluster of one or more appliances. The join operation copies configuration information to the new appliance that you are adding, including certificate, SSO, licensing, database, and messaging information.

You must add appliances to a cluster one at a time and not in parallel.

Prerequisites

- You must have one or more vRealize Automation appliance nodes already in the cluster, where one node is the primary node. See [“Configure the Primary vRealize Automation Appliance,”](#) on page 68.
You can set a new node to be the primary node only after joining the new node to the cluster.
- Verify that the load balancer is configured for use with the new vRealize Automation appliance.
- Verify that traffic can pass through the load balancer to reach all current nodes and the new node that you are about to add.
- Enable time synchronization on the new node. See [“Enable Time Synchronization on the vRealize Automation Appliance,”](#) on page 72.
- Verify that all vRealize Automation services have started, on the existing cluster appliance nodes and the new node that you are adding.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
- 2 Continue past any certificate warnings.
- 3 Log in with user name root and the password you specified when deploying the vRealize Automation appliance.
- 4 Select **vRA Settings > Cluster**.
- 5 Enter the FQDN of a previously configured vRealize Automation appliance in the **Leading Cluster Node** text box.
You can use the FQDN of the primary vRealize Automation appliance, or any vRealize Automation appliance that is already joined to the cluster.
- 6 Type the root password in the **Password** text box.
- 7 Click **Join Cluster**.
- 8 Continue past any certificate warnings.
Services for the cluster are restarted.
- 9 Verify that services are running.
 - a Click the **Services** tab.
 - b Click the **Refresh** tab to monitor the progress of service startup.

Disable Unused Services

To conserve internal resources in cases where an external instance of vRealize Orchestrator is used, you may disable the embedded vRealize Orchestrator service.

Prerequisites

[“Add Another vRealize Automation Appliance to the Cluster,”](#) on page 72

Procedure

- 1 Log in to the vRealize Automation appliance console.
- 2 Stop the vRealize Orchestrator service.

```
service vco-server stop
chkconfig vco-server off
```

Validate the Distributed Deployment

After deploying additional instances of the vRealize Automation appliance, you validate that you can access the clustered appliances.

Procedure

- 1 In the load balancer management interface or configuration file, temporarily disable all nodes except the node that you are testing.
- 2 Confirm that you can log in to vRealize Automation through the load balancer address:
<https://vrealize-automation-appliance-load-balancer-FQDN/vcac>
- 3 After verifying that you can access the new vRealize Automation appliance through the load balancer, re-enable the other nodes.

Install the IaaS Components in a Distributed Configuration

The system administrator installs the IaaS components after the appliances are deployed and fully configured. The IaaS components provide access to vRealize Automation Infrastructure features.

All components must run under the same service account user, which must be a domain account that has privileges on each distributed IaaS server. Do not use local system accounts.

Prerequisites

- [“Configure the Primary vRealize Automation Appliance,”](#) on page 68.
- If your site includes multiple instances of vRealize Automation appliance, [“Add Another vRealize Automation Appliance to the Cluster,”](#) on page 72.
- Verify that your installation servers meet the requirements described in [“IaaS Web Service and Model Manager Server Requirements,”](#) on page 22.
- Obtain a certificate from a trusted certificate authority for import to the trusted root certificate store of the machines on which you intend to install the Component Website and Model Manager data.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

- 1 [Install IaaS Certificates](#) on page 75
 For production environments, obtain a domain certificate from a trusted certificate authority. Import the certificate to the trusted root certificate store of all machines on which you intend to install the Website Component and Manager Service (the IIS machines) during the IaaS installation.
- 2 [Download the vRealize Automation IaaS Installer](#) on page 76
 To install IaaS on your distributed virtual or physical Windows servers, you download a copy of the IaaS installer from the vRealize Automation appliance.
- 3 [Choosing an IaaS Database Scenario](#) on page 77
 vRealize Automation IaaS uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies.
- 4 [Install an IaaS Website Component and Model Manager Data](#) on page 81
 The system administrator installs the Website component to provide access to infrastructure capabilities in the vRealize Automation web console. You can install one or many instances of the Website component, but you must configure Model Manager Data on the machine that hosts the first Website component. You install Model Manager Data only once.

- 5 [Install Additional IaaS Web Server Components](#) on page 85
The Web server provides access to infrastructure capabilities in vRealize Automation. After the first Web server is installed, you might increase performance by installing additional IaaS Web servers.
- 6 [Install the Active Manager Service](#) on page 87
The active Manager Service is a Windows service that coordinates communication between IaaS Distributed Execution Managers, the database, agents, proxy agents, and SMTP.
- 7 [Install a Backup Manager Service Component](#) on page 90
The backup Manager Service provides redundancy and high availability, and may be started manually if the active service stops.
- 8 [Installing Distributed Execution Managers](#) on page 92
You install the Distributed Execution Manager as one of two roles: DEM Orchestrator or DEM Worker. You must install at least one DEM instance for each role, and you can install additional DEM instances to support failover and high-availability.
- 9 [Configuring Windows Service to Access the IaaS Database](#) on page 95
A system administrator can change the authentication method used to access the SQL database during run time (after the installation is complete). By default, the Windows identity of the currently logged on account is used to connect to the database after it is installed.
- 10 [Verify IaaS Services](#) on page 97
After installation, the system administrator verifies that the IaaS services are running. If the services are running, the installation is a success.

What to do next

Install a DEM Orchestrator and at least one DEM Worker instance. See [“Installing Distributed Execution Managers,”](#) on page 92.

Install IaaS Certificates

For production environments, obtain a domain certificate from a trusted certificate authority. Import the certificate to the trusted root certificate store of all machines on which you intend to install the Website Component and Manager Service (the IIS machines) during the IaaS installation.

Prerequisites

On Windows 2012 machines, you must disable TLS1.2 for certificates that use SHA512. For more information about disabling TLS1.2, see [Microsoft Knowledge Base article 245030](#).

Procedure

- 1 Obtain a certificate from a trusted certificate authority.
- 2 Open the Internet Information Services (IIS) Manager.
- 3 Double-click **Server Certificates** from Features View.
- 4 Click **Import** in the Actions pane.
 - a Enter a file name in the **Certificate file** text box, or click the browse button (...), to navigate to the name of a file where the exported certificate is stored.
 - b Enter a password in the **Password** text box if the certificate was exported with a password.
 - c Select **Mark this key as exportable**.
- 5 Click **OK**.
- 6 Click on the imported certificate and select **View**.

- 7 Verify that the certificate and its chain is trusted.

If the certificate is untrusted, you see the message, *This CA root certificate is not trusted.*

NOTE You must resolve the trust issue before proceeding with the installation. If you continue, your deployment fails.

- 8 Restart IIS or open an elevated command prompt window and type `iisreset`.

What to do next

[“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Download the vRealize Automation IaaS Installer

To install IaaS on your distributed virtual or physical Windows servers, you download a copy of the IaaS installer from the vRealize Automation appliance.

If you see certificate warnings during this process, continue past them to finish the installation.

Prerequisites

- [“Configure the Primary vRealize Automation Appliance,”](#) on page 68 and, optionally, [“Add Another vRealize Automation Appliance to the Cluster,”](#) on page 72.
- Verify that your installation servers meet the requirements described in [“IaaS Web Service and Model Manager Server Requirements,”](#) on page 22.
- Verify that you imported a certificate to IIS and that the certificate root or the certificate authority is in the trusted root on the installation machine.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

- 1 (Optional) Activate HTTP if you are installing on a Windows 2012 machine.
 - a Select **Features > Add Features** from Server Manager.
 - b Expand **WCF Services** under .NET Framework Features.
 - c Select **HTTP Activation**.
- 2 Log in to the IaaS Windows server using an account that has administrator rights.
- 3 Open a Web browser directly to the vRealize Automation appliance installer URL. Do not use a load balancer address.

`https://vrealize-automation-appliance-FQDN:5480/installer`
- 4 Click **IaaS Installer**.
- 5 Save `setup__vrealize-automation-appliance-FQDN@5480` to the Windows server.

Do not change the installer file name. It is used to connect the installation to the vRealize Automation appliance.
- 6 Download the installer file to each IaaS Windows server on which you are installing components.

What to do next

Install an IaaS database, see [“Choosing an IaaS Database Scenario,”](#) on page 77.

Choosing an IaaS Database Scenario

vRealize Automation IaaS uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies.

Depending on your preferences and privileges, there are several procedures to choose from to create the IaaS database.

NOTE You can enable secure SSL when creating or upgrading the SQL database. For example, when you create or upgrade the SQL database, you can use the Secure SSL option to specify that the SSL configuration which is already specified in the SQL server be enforced when connecting to the SQL database. SSL provides a more secure connection between the IaaS server and SQL database. This option, which is available in the custom installation wizard, requires that you have already configured SSL on the SQL server. For related information about configuring SSL on the SQL server, see [Microsoft Knowledge Base article 316898](#).

Table 4-10. Choosing an IaaS Database Scenario

Scenario	Procedure
Create the IaaS database manually using the provided database scripts. This option enables a database administrator to review the changes carefully before creating the database.	“Create the IaaS Database Manually,” on page 77.
Prepare an empty database and use the installer to populate the database schema. This option enables the installer to use a database user with dbo privileges to populate the database, instead of requiring sysadmin privileges.	“Prepare an Empty Database,” on page 78.
Use the installer to create the database. This is the simplest option but requires the use of sysadmin privileges in the installer.	“Create the IaaS Database Using the Installation Wizard,” on page 79.

Create the IaaS Database Manually

The vRealize Automation system administrator can create the database manually using VMware-provided scripts.

Prerequisites

- Microsoft .NET Framework 4.5.2 or later must be installed on the SQL Server host.
- Use Windows Authentication, rather than SQL Authentication, to connect to the database.
- Verify the database installation prerequisites. See [“IaaS Database Server Requirements,”](#) on page 21.
- Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.

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

Procedure

- 1 Navigate to the Database subdirectory in the directory where you extracted the installation zip archive.
- 2 Extract the DBInstall.zip archive to a local directory.
- 3 Log in to the Windows database host with sufficient rights to create and drop databases **sysadmin** privileges in the SQL Server instance.

- Review the database deployment scripts as needed. In particular, review the settings in the DBSettings section of CreateDatabase.sql and edit them if necessary.

The settings in the script are the recommended settings. Only ALLOW_SNAPSHOT_ISOLATION ON and READ_COMMITTED_SNAPSHOT ON are required.

- Execute the following command with the arguments described in the table.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Table 4-11. Database Values

Variable	Value
<i>db_server</i>	Specifies the SQL Server instance in the format <code>dbhostname[,port number]\SQL instance</code> . Specify a port number only if you are using a non-default port. The Microsoft SQL default port number is 1433. The default value for <i>db_server</i> is <code>localhost</code> .
<i>db_name</i>	Name of the database. The default value is <code>vra</code> . Database names must consist of no more than 128 ASCII characters.
<i>db_dir</i>	Path to the data directory for the database, excluding the final slash.
<i>log_dir</i>	Path to the log directory for the database, excluding the final slash.
<i>service_user</i>	User name under which the Manager Service runs.
<i>Web_user</i>	User name under which the Web services run.
<i>version_string</i>	The vRealize Automation version, found by logging in to the vRealize Automation appliance and clicking the Update tab. For example, the vRealize Automation 6.1 version string is <code>6.1.0.1200</code> .

The database is created.

What to do next

[“Install the IaaS Components in a Distributed Configuration,”](#) on page 74.

Prepare an Empty Database

A vRealize Automation system administrator can install the IaaS schema on an empty database. This installation method provides maximum control over database security.

Prerequisites

- Verify the database installation prerequisites. See [“IaaS Database Server Requirements,”](#) on page 21.
- Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.

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

Procedure

- Navigate to the Database directory within the directory where you extracted the installation zip archive.
- Extract the DBInstall.zip archive to a local directory.

- 3 Log in to the Windows database host with **sysadmin** privileges within the SQL Server instance.
- 4 Edit `CreateDatabase.sql` and replace all instances of the variables in the table with the correct values for your environment.

Table 4-12. Database Values

Variable	Value
<code>\$(DBName)</code>	Name of the database, such as <code>vra</code> . Database names must consist of no more than 128 ASCII characters.
<code>\$(DBDir)</code>	Path to the data directory for the database, excluding the final slash.
<code>\$(LogDir)</code>	Path to the log directory for the database, excluding the final slash.

- 5 Review the settings in the `DB Settings` section of `CreateDatabase.sql` and edit them if needed.

The settings in the script are the recommended settings for the IaaS database. Only `ALLOW_SNAPSHOT_ISOLATION ON` and `READ_COMMITTED_SNAPSHOT ON` are required.

- 6 Open SQL Server Management Studio.

- 7 Click **New Query**.

An SQL Query window opens.

- 8 On the **Query** menu, ensure that **SQLCMD Mode** is selected.

- 9 Paste the entire modified contents of `CreateDatabase.sql` into the query pane.

- 10 Click **Execute**.

The script runs and creates the database.

What to do next

[“Install the IaaS Components in a Distributed Configuration,”](#) on page 74.

Create the IaaS Database Using the Installation Wizard

vRealize Automation uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies.

The following steps describe how to create the IaaS database using the installer or populate an existing empty database. It is also possible to create the database manually. See [“Create the IaaS Database Manually,”](#) on page 77.

Prerequisites

- If you are creating the database with Windows authentication, instead of SQL authentication, verify that the user who runs the installer has **sysadmin** rights on the SQL server.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.

- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Click **Next**.
- 6 Select **Custom Install** on the Installation Type page.
- 7 Select **IaaS Server** under Component Selection on the Installation Type page.
- 8 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 9 Click **Next**.
- 10 On the IaaS Server Custom Install page, select **Database**.
- 11 In the **Database Instance** text box, specify the database instance or click **Scan** and select from the list of instances. If the database instance is on a non-default port, include the port number in instance specification by using the form *dbhost,SQL_port_number\SQLinstance*. The Microsoft SQL default port number is 1443.
- 12 (Optional) Select the **Use SSL for database connection** checkbox.
By default, the checkbox is enabled. SSL provides a more secure connection between the IaaS server and SQL database. However, you must first configure SSL on the SQL server to support this option. For more about configuring SSL on the SQL server, see [Microsoft Knowledge Base article 316898](#).
- 13 Choose your database installation type from the **Database Name** panel.
 - Select **Use existing empty database** to create the schema in an existing database.
 - Enter a new database name or use the default name **vra** to create a new database. Database names must consist of no more than 128 ASCII characters.
- 14 Deselect **Use default data and log directories** to specify alternative locations or leave it selected to use the default directories (recommended).
- 15 Select an authentication method for installing the database from the **Authentication** list.
 - To use the credentials under which you are running the installer to create the database, select **User Windows identity...**
 - To use SQL authentication, deselect **Use Windows identity...** Type SQL credentials in the user and password text boxes.

By default, the Windows service user account is used during runtime access to the database, and must have sysadmin rights to the SQL Server instance. The credentials used to access the database at runtime can be configured to use SQL credentials.

Windows authentication is recommended. When you choose SQL authentication, the unencrypted database password appears in certain configuration files.

- 16 Click **Next**.
- 17 Complete the Prerequisite Check.

Option	Description
No errors	Click Next .
Noncritical errors	Click Bypass .
Critical errors	Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click Check Again to verify.

- 18 Click **Install**.
- 19 When the success message appears, deselect **Guide me through initial configuration** and click **Next**.
- 20 Click **Finish**.

The database is ready for use.

Install an IaaS Website Component and Model Manager Data

The system administrator installs the Website component to provide access to infrastructure capabilities in the vRealize Automation web console. You can install one or many instances of the Website component, but you must configure Model Manager Data on the machine that hosts the first Website component. You install Model Manager Data only once.

Prerequisites

- Install the IaaS Database, see [“Choosing an IaaS Database Scenario,”](#) on page 77.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See [“Security Passphrase,”](#) on page 31.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

- 1 [Install the First IaaS Web Server Component](#) on page 81
You install the IaaS Web server component to provide access to infrastructure capabilities in vRealize Automation.
- 2 [Configure Model Manager Data](#) on page 83
You install the Model Manager component on the same machine that hosts the first Web server component. You only install Model Manager Data once.

You can install additional Website components or install the Manager Service. See [“Install Additional IaaS Web Server Components,”](#) on page 85 or [“Install the Active Manager Service,”](#) on page 87.

Install the First IaaS Web Server Component

You install the IaaS Web server component to provide access to infrastructure capabilities in vRealize Automation.

You can install multiple IaaS Web servers, but only the first one includes Model Manager Data.

Prerequisites

- [“Create the IaaS Database Using the Installation Wizard,”](#) on page 79.
- Verify that your environment meets the requirements described in [“IaaS Web Service and Model Manager Server Requirements,”](#) on page 22.

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “[Security Passphrase](#),” on page 31.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

- 1 If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.

In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.
- 2 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 3 Click **Next**.
- 4 Accept the license agreement and click **Next**.
- 5 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.

The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.

Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 6 Click **Next**.
- 7 Select **Custom Install** on the Installation Type page.
- 8 Select **IaaS Server** under Component Selection on the Installation Type page.
- 9 Accept the root install location or click **Change** and select an installation path.

Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.

If you install more than one IaaS component, always install them to the same path.
- 10 Click **Next**.
- 11 Select **Website** and **ModelManagerData** on the IaaS Server Custom Install page.
- 12 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.
- 13 Type an available port number in the **Port number** text box, or accept the default port 443.
- 14 Click **Test Binding** to confirm that the port number is available for use.

- 15 Select the certificate for this component.
 - a If you imported a certificate after you began the installation, click **Refresh** to update the list.
 - b Select the certificate to use from **Available certificates**.
 - c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

If you are installing in an environment that does not use load balancers, you can select **Generate a Self-Signed Certificate** instead of selecting a certificate. If you are installing additional Web site components behind a load balancer, do not generate self-signed certificates. Import the certificate from the main IaaS Web server to ensure that you use the same certificate on all servers behind the load balancer.

- 16 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.
- 17 (Optional) Select **Suppress certificate mismatch** to suppress certificate errors. The installation ignores certificate name mismatch errors as well as any remote certificate-revocation list match errors.

This is a less secure option.

Configure Model Manager Data

You install the Model Manager component on the same machine that hosts the first Web server component. You only install Model Manager Data once.

Prerequisites

[“Install the First IaaS Web Server Component,”](#) on page 81.

Procedure

- 1 Click the **Model Manager Data** tab.
- 2 In the **Server** text box, enter the vRealize Automation appliance fully qualified domain name.
vrealize-automation-appliance.mycompany.com
Do not enter an IP address.
- 3 Click **Load** to display the **SSO Default Tenant**.
The `vsphere.local` default tenant is created automatically when you configure single sign-on. Do not modify it.
- 4 Click **Download** to import the certificate from the virtual appliance.
It might take several minutes to download the certificate.
- 5 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.
- 6 Click **Accept Certificate**.
- 7 Type `administrator@vsphere.local` in the **User name** text box and the password you created when you configured the SSO in the **Password** and **Confirm** text boxes.
- 8 (Optional) Click **Test** to verify the credentials.

- 9 In the **IaaS Server** text box, identify the IaaS Web server component.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the IaaS Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the IaaS Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 10 Click **Test** to verify the server connection.
- 11 Click **Next**.
- 12 Complete the Prerequisite Check.

Option	Description
No errors	Click Next .
Noncritical errors	Click Bypass .
Critical errors	Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click Check Again to verify.

- 13 On the Server and Account Settings page, in the **Server Installation Information** text boxes, enter the user name and password of the service account user that has administrative privileges on the current installation server.

The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.

- 14 Provide the passphrase used to generate the encryption key that protects the database.

Option	Description
If you have already installed components in this environment	Type the passphrase you created previously in the Passphrase and Confirm text boxes.
If this is the first installation	Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.

Keep this passphrase in a secure place for later use.

- 15 Specify the IaaS database server, database name, and authentication method for the database server in the **Microsoft SQL Database Installation Information** text box.

This is the IaaS database server, name, and authentication information that you created previously.

- 16 Click **Next**.
- 17 Click **Install**.
- 18 When the installation finishes, deselect **Guide me through the initial configuration** and click **Next**.

What to do next

You can install additional Web server components or install the Manager Service. See [“Install Additional IaaS Web Server Components,”](#) on page 85 or [“Install the Active Manager Service,”](#) on page 87.

Install Additional IaaS Web Server Components

The Web server provides access to infrastructure capabilities in vRealize Automation. After the first Web server is installed, you might increase performance by installing additional IaaS Web servers.

Do not install Model Manager Data with an additional Web server component. Only the first Web server component hosts Model Manager Data.

Prerequisites

- [“Install an IaaS Website Component and Model Manager Data,”](#) on page 81.
- Verify that your environment meets the requirements described in [“IaaS Web Service and Model Manager Server Requirements,”](#) on page 22.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See [“Security Passphrase,”](#) on page 31.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

- 1 If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.

In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.
- 2 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 3 Click **Next**.
- 4 Accept the license agreement and click **Next**.
- 5 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.

Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 6 Click **Next**.
- 7 Select **Custom Install** on the Installation Type page.
- 8 Select **IaaS Server** under Component Selection on the Installation Type page.
- 9 Accept the root install location or click **Change** and select an installation path.

Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.

If you install more than one IaaS component, always install them to the same path.
- 10 Click **Next**.

- 11 Select **Website** on the IaaS Server Custom Install page.
- 12 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.
- 13 Type an available port number in the **Port number** text box, or accept the default port 443.
- 14 Click **Test Binding** to confirm that the port number is available for use.
- 15 Select the certificate for this component.
 - a If you imported a certificate after you began the installation, click **Refresh** to update the list.
 - b Select the certificate to use from **Available certificates**.
 - c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

If you are installing in an environment that does not use load balancers, you can select **Generate a Self-Signed Certificate** instead of selecting a certificate. If you are installing additional Web site components behind a load balancer, do not generate self-signed certificates. Import the certificate from the main IaaS Web server to ensure that you use the same certificate on all servers behind the load balancer.

- 16 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.
- 17 (Optional) Select **Suppress certificate mismatch** to suppress certificate errors. The installation ignores certificate name mismatch errors as well as any remote certificate-revocation list match errors.

This is a less secure option.

- 18 In the **IaaS Server** text box, identify the first IaaS Web server component.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the IaaS Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the IaaS first Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 19 Click **Test** to verify the server connection.
- 20 Click **Next**.
- 21 Complete the Prerequisite Check.

Option	Description
No errors	Click Next .
Noncritical errors	Click Bypass .
Critical errors	Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click Check Again to verify.

- 22 On the Server and Account Settings page, in the **Server Installation Information** text boxes, enter the user name and password of the service account user that has administrative privileges on the current installation server.

The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.

- 23 Provide the passphrase used to generate the encryption key that protects the database.

Option	Description
If you have already installed components in this environment	Type the passphrase you created previously in the Passphrase and Confirm text boxes.
If this is the first installation	Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.

Keep this passphrase in a secure place for later use.

- 24 Specify the IaaS database server, database name, and authentication method for the database server in the **Microsoft SQL Database Installation Information** text box.

This is the IaaS database server, name, and authentication information that you created previously.

- 25 Click **Next**.
- 26 Click **Install**.
- 27 When the installation finishes, deselect **Guide me through the initial configuration** and click **Next**.

What to do next

[“Install the Active Manager Service,”](#) on page 87.

Install the Active Manager Service

The active Manager Service is a Windows service that coordinates communication between IaaS Distributed Execution Managers, the database, agents, proxy agents, and SMTP.

Your IaaS deployment requires that only one Windows machine actively run the Manager Service. For backup or high availability, you may deploy additional Windows machines where you manually start the Manager Service if the active service stops.

IMPORTANT Simultaneously running an active Manager Service on multiple IaaS Windows servers makes vRealize Automation unusable.

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See [“Security Passphrase,”](#) on page 31.
- (Optional) If you want to install the Manager Service in a Website other than the default Website, first create a Website in Internet Information Services.
- Microsoft .NET Framework 4.5.2 is installed.
- Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.
- Verify that the Website load balancer is configured and that the timeout value for the load balancer is set to a minimum of 180 seconds.
- [“Install an IaaS Website Component and Model Manager Data,”](#) on page 81.

Procedure

- 1 If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.

In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.

- 2 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Click **Next**.
- 6 Select **Custom Install** on the Installation Type page.
- 7 Select **IaaS Server** under Component Selection on the Installation Type page.
- 8 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 9 Click **Next**.
- 10 Select **Manager Service** on the IaaS Server Custom Install page.
- 11 In the **IaaS Server** text box, identify the IaaS Web server component.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the IaaS Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the IaaS Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 12 Select **Active node with startup type set to automatic**.
- 13 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.
- 14 Type an available port number in the **Port number** text box, or accept the default port 443.
- 15 Click **Test Binding** to confirm that the port number is available for use.

- 16 Select the certificate for this component.
 - a If you imported a certificate after you began the installation, click **Refresh** to update the list.
 - b Select the certificate to use from **Available certificates**.
 - c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

If you are installing in an environment that does not use load balancers, you can select **Generate a Self-Signed Certificate** instead of selecting a certificate. If you are installing additional Web site components behind a load balancer, do not generate self-signed certificates. Import the certificate from the main IaaS Web server to ensure that you use the same certificate on all servers behind the load balancer.

- 17 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.
- 18 Click **Next**.
- 19 Check the prerequisites and click **Next**.
- 20 On the Server and Account Settings page, in the **Server Installation Information** text boxes, enter the user name and password of the service account user that has administrative privileges on the current installation server.

The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.

- 21 Provide the passphrase used to generate the encryption key that protects the database.

Option	Description
If you have already installed components in this environment	Type the passphrase you created previously in the Passphrase and Confirm text boxes.
If this is the first installation	Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.

Keep this passphrase in a secure place for later use.

- 22 Specify the IaaS database server, database name, and authentication method for the database server in the **Microsoft SQL Database Installation Information** text box.

This is the IaaS database server, name, and authentication information that you created previously.
- 23 Click **Next**.
- 24 Click **Install**.
- 25 When the installation finishes, deselect **Guide me through the initial configuration** and click **Next**.
- 26 Click **Finish**.

What to do next

- To ensure that the Manager Service you installed is the active instance, verify that the vCloud Automation Center Service is running and set it to "Automatic" startup type.
- You can install another instance of the Manager Service component as a passive backup that you can start manually if the active instance fails. See "[Install a Backup Manager Service Component](#)," on page 90.
- A system administrator can change the authentication method used to access the SQL database during run time (after the installation is complete). See "[Configuring Windows Service to Access the IaaS Database](#)," on page 95.

Install a Backup Manager Service Component

The backup Manager Service provides redundancy and high availability, and may be started manually if the active service stops.

Your IaaS deployment requires that only one Windows machine actively run the Manager Service. Machines that provide the backup Manager Service must have the service stopped and configured to start manually.

IMPORTANT Simultaneously running an active Manager Service on multiple IaaS Windows servers makes vRealize Automation unusable.

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See [“Security Passphrase,”](#) on page 31.
- (Optional) If you want to install the Manager Service in a Web site other than the default Web site, first create a Web site in Internet Information Services.
- Microsoft .NET Framework 4.5.2 is installed.
- Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.
- Verify that the Website load balancer is configured.
- [“Install an IaaS Website Component and Model Manager Data,”](#) on page 81.

Procedure

- 1 If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.

In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.
- 2 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 3 Click **Next**.
- 4 Accept the license agreement and click **Next**.
- 5 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.

The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.

Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 6 Click **Next**.
- 7 Select **Custom Install** on the Installation Type page.
- 8 Select **IaaS Server** under Component Selection on the Installation Type page.

- 9 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 10 Click **Next**.
- 11 Select **Manager Service** on the IaaS Server Custom Install page.
- 12 In the **IaaS Server** text box, identify the IaaS Web server component.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the IaaS Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the IaaS Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 13 Select **Disaster recovery cold standby node**.
- 14 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.
- 15 Type an available port number in the **Port number** text box, or accept the default port 443.
- 16 Click **Test Binding** to confirm that the port number is available for use.
- 17 Select the certificate for this component.
 - a If you imported a certificate after you began the installation, click **Refresh** to update the list.
 - b Select the certificate to use from **Available certificates**.
 - c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

If you are installing in an environment that does not use load balancers, you can select **Generate a Self-Signed Certificate** instead of selecting a certificate. If you are installing additional Web site components behind a load balancer, do not generate self-signed certificates. Import the certificate from the main IaaS Web server to ensure that you use the same certificate on all servers behind the load balancer.
- 18 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.
- 19 Click **Next**.
- 20 Check the prerequisites and click **Next**.
- 21 On the Server and Account Settings page, in the **Server Installation Information** text boxes, enter the user name and password of the service account user that has administrative privileges on the current installation server.
The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.

- 22 Provide the passphrase used to generate the encryption key that protects the database.

Option	Description
If you have already installed components in this environment	Type the passphrase you created previously in the Passphrase and Confirm text boxes.
If this is the first installation	Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.

Keep this passphrase in a secure place for later use.

- 23 Specify the IaaS database server, database name, and authentication method for the database server in the **Microsoft SQL Database Installation Information** text box.

This is the IaaS database server, name, and authentication information that you created previously.

- 24 Click **Next**.
- 25 Click **Install**.
- 26 When the installation finishes, deselect **Guide me through the initial configuration** and click **Next**.
- 27 Click **Finish**.

What to do next

- To ensure that the Manager Service you installed is a passive backup instance, verify that the vRealize Automation Service is not running and set it to "Manual" startup type.
- A system administrator can change the authentication method used to access the SQL database during run time (after the installation is complete). See [“Configuring Windows Service to Access the IaaS Database,”](#) on page 95.

Installing Distributed Execution Managers

You install the Distributed Execution Manager as one of two roles: DEM Orchestrator or DEM Worker. You must install at least one DEM instance for each role, and you can install additional DEM instances to support failover and high-availability.

The system administrator must choose installation machines that meet predefined system requirements. The DEM Orchestrator and the Worker can reside on the same machine.

As you plan to install Distributed Execution Managers, keep in mind the following considerations:

- DEM Orchestrators support active-active high availability. Typically, you install one DEM Orchestrator on each Manager Service machine.
- Install the Orchestrator on a machine with strong network connectivity to the Model Manager host.
- Install a second DEM Orchestrator on a different machine for failover.
- Typically, you install DEM Workers on the IaaS Manager Service server or on a separate server. The server must have network connectivity to the Model Manager host.
- You can install additional DEM instances for redundancy and scalability, including multiple instances on the same machine.

There are specific requirements for the DEM installation that depend on the endpoints you use. See [“Distributed Execution Manager Requirements,”](#) on page 23.

Install the Distributed Execution Managers

You must install at least one DEM Worker and one DEM Orchestrator. The installation procedure is the same for both roles.

DEM Orchestrators support active-active high availability. Typically, you install a single DEM Orchestrator on each Manager Service machine. You can install DEM Orchestrators and DEM workers on the same machine.

Prerequisites

[“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Click **Next**.
- 6 Select **Custom Install** on the Installation Type page.
- 7 Select **Distributed Execution Managers** under Component Selection on the Installation Type page.
- 8 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 9 Click **Next**.
- 10 Check prerequisites and click **Next**.
- 11 Enter the log in credentials under which the service will run.
The service account must have local administrator privileges and be the domain account that you have been using throughout IaaS installation. The service account has privileges on each distributed IaaS server and must not be a local system account.
- 12 Click **Next**.

- 13 Select the installation type from the **DEM role** drop-down menu.

Option	Description
Worker	The Worker executes workflows.
Orchestrator	The Orchestrator oversees DEM worker activities, including scheduling and preprocessing workflows, and monitors DEM worker online status.

- 14 Enter a unique name that identifies this DEM in the **DEM name** text box.

If you plan to use the migration tool, this name must exactly match the name you used in your vCloud Automation Center 5.2.3 installation. The name cannot include spaces and cannot exceed 128 characters. If you enter a previously used name, the following message appears: "DEM name already exists. To enter a different name for this DEM, click Yes. If you are restoring or reinstalling a DEM with the same name, click No."

- 15 (Optional) Enter a description of this instance in **DEM description**.
- 16 Enter the host names and ports in the **Manager Service Host name** and **Model Manager Web Service Host name** text boxes.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancers for the Manager Service component and the Web server that hosts Model Manager, <i>mgr-svc-load-balancer.mycompany.com:443</i> and <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component and the Web server that hosts Model Manager, <i>mgr-svc.mycompany.com:443</i> and <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 17 (Optional) Click **Test** to test the connections to the Manager Service and Model Manager Web Service.
- 18 Click **Add**.
- 19 Click **Next**.
- 20 Click **Install**.
- 21 When the installation finishes, deselect **Guide me through the initial configuration** and click **Next**.
- 22 Click **Finish**.

What to do next

- Verify that the service is running and that the log shows no errors. The service name is VMware DEM *Role - Name* where role is Orchestrator or Worker. The log location is *Install Location*\Distributed Execution Manager\Name\Log.
- Repeat this procedure to install additional DEM instances.

Configure the DEM to Connect to SCVMM at a Different Installation Path

By default, the DEM Worker configuration file uses the default installation path of Microsoft System Center Virtual Machine Manager (SCVMM) 2012 console. You must update the configuration when the SCVMM console is installed to another location.

This release supports the SCVMM 2012 R2 console, so you must update the path to 2012 R2. You also might need to update the path if you installed the SCVMM console to a non-default path.

You only need this procedure if you have SCVMM endpoints and agents.

Prerequisites

- Know the actual path where the SCVMM console is installed.

The following is the default 2012 path that you must replace in the configuration file.

```
path="{ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin"
```

Procedure

- 1 Stop the DEM Worker service.
- 2 Open the following file in a text editor.
Program Files (x86)\VMware\VCAC\Distributed Execution Manager*instance-name*\DynamicOps.DEM.exe.config
- 3 Locate the <assemblyLoadConfiguration> section.
- 4 Update each path, using the following example as a guideline.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="{ProgramFiles}\Microsoft
System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
    <add name="TraceWrapper" path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual
Machine Manager\bin"/>
    <add name="Utils" path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 Save and close DynamicOps.DEM.exe.config.
- 6 Restart the DEM Worker service.

For more information, see [“SCVMM Requirements,”](#) on page 25.

Additional information about preparing the SCVMM environment and creating an SCVMM endpoint is available in *Configuring vRealize Automation*.

Configuring Windows Service to Access the IaaS Database

A system administrator can change the authentication method used to access the SQL database during run time (after the installation is complete). By default, the Windows identity of the currently logged on account is used to connect to the database after it is installed.

Enable IaaS Database Access from the Service User

If the SQL database is installed on a separate host from the Manager Service, database access from the Manager Service must be enabled. If the user name under which the Manager Service will run is the owner of the database, no action is required. If the user is not the owner of the database, the system administrator must grant access.

Prerequisites

- [“Choosing an IaaS Database Scenario,”](#) on page 77.
- Verify that the user name under which the Manager Service will run is not the owner of the database.

Procedure

- 1 Navigate to the `Database` subdirectory within the directory where you extracted the installation zip archive.
- 2 Extract the `DBInstall.zip` archive to a local directory.
- 3 Log in to the database host as a user with the `sysadmin` role in the SQL Server instance.
- 4 Edit `VMPSOpsUser.sql` and replace all instances of `$(Service User)` with user (from Step 3) under which the Manager Service will run.

Do not replace `ServiceUser` in the line ending with `WHERE name = N'ServiceUser'`.

- 5 Open SQL Server Management Studio.
- 6 Select the database (vCAC by default) in **Databases** in the left-hand pane.
- 7 Click **New Query**.
The SQL Query window opens in the right-hand pane.
- 8 Paste the modified contents of `VMPSOpsUser.sql` into the query window.
- 9 Click **Execute**.

Database access is enabled from the Manager Service.

Configure the Windows Services Account to Use SQL Authentication

By default, the Windows service account accesses the database during run-time, even if you configured the database for SQL authentication. You can change run-time authentication from Windows to SQL.

One reason to change run-time authentication might be when, for example, the database is on an untrusted domain.

Prerequisites

Verify that the vRealize Automation SQL Server database exists. Begin with [“Choosing an IaaS Database Scenario,”](#) on page 77.

Procedure

- 1 Using an account with administrator privileges, log in to the IaaS Windows server that hosts the Manager Service.
- 2 In **Administrative Tools > Services**, stop the **VMware vCloud Automation Center** service.
- 3 Open the following files in a text editor.
 - C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config
 - C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
- 4 In each file, locate the `<connectionStrings>` section.

- 5 Replace


```
Integrated Security=True;
```

 with


```
User Id=database-username;Password=database-password;
```
- 6 Save and close the files.


```
ManagerService.exe.config
```

```
Web.config
```
- 7 Start the **VMware vCloud Automation Center** service.
- 8 Use the `iisreset` command to restart IIS.

Verify IaaS Services

After installation, the system administrator verifies that the IaaS services are running. If the services are running, the installation is a success.

Procedure

- 1 From the Windows desktop of the IaaS machine, select **Administrative Tools > Services**.
- 2 Locate the following services and verify that their status is Started and the Startup Type is set to Automatic.
 - VMware DEM – Orchestrator – *Name* where *Name* is the string provided in the **DEM Name** box during installation.
 - VMware DEM – Worker – *Name* where *Name* is the string provided in the **DEM Name** box during installation.
 - VMware vCloud Automation Center *Agent name*
 - VMware vCloud Automation Center Service
- 3 Close the **Services** window.

Installing vRealize Automation Agents

vRealize Automation uses agents to integrate with external systems. A system administrator can select agents to install to communicate with other virtualization platforms.

vRealize Automation uses the following types of agents to manage external systems:

- Hypervisor proxy agents (vSphere, Citrix Xen Servers and Microsoft Hyper-V servers)
- External provisioning infrastructure (EPI) integration agents
- Virtual Desktop Infrastructure (VDI) agents
- Windows Management Instrumentation (WMI) agents

For high-availability, you can install multiple agents for a single endpoint. Install each redundant agent on a separate server, but name and configure them identically. Redundant agents provide some fault tolerance, but do not provide failover. For example, if you install two vSphere agents, one on server A and one on server B, and server A becomes unavailable, the agent installed on server B continues to process work items. However, the server B agent cannot finish processing a work item that the server A agent had already started.

You have the option to install a vSphere agent as part of your minimal installation, but after the installation you can also add other agents, including an additional vSphere agent. In a distributed deployment, you install all your agents after you complete the base distributed installation. The agents you install depend on the resources in your infrastructure.

For information about using vSphere agents, see [“vSphere Agent Requirements,”](#) on page 99.

Set the PowerShell Execution Policy to RemoteSigned

You must set the PowerShell Execution Policy from Restricted to RemoteSigned or Unrestricted to allow local PowerShell scripts to be run.

For more information about the PowerShell Execution Policy, see [Microsoft Technet article hh847748](#). If your PowerShell Execution Policy is managed at the group policy level, contact your IT support for about their restrictions on policy changes, and see [Microsoft Technet article jj149004](#).

Prerequisites

- Log in as a Windows administrator.
- Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.
- For more information about PowerShell Execution Policy, run `help about_signing` or `help Set-ExecutionPolicy` at the PowerShell command prompt.

Procedure

- 1 Select **Start > All Programs > Windows PowerShell version > Windows PowerShell**.
- 2 For Remote Signed, run `Set-ExecutionPolicy RemoteSigned`.
- 3 For Unrestricted, run `Set-ExecutionPolicy Unrestricted`.
- 4 Verify that the command did not produce any errors.
- 5 Type **Exit** at the PowerShell command prompt.

Choosing the Agent Installation Scenario

The agents that you need to install depend on the external systems with which you plan to integrate.

Table 4-13. Choosing an Agent Scenario

Integration Scenario	Agent Requirements and Procedures
Provision cloud machines by integrating with a cloud environment such as Amazon Web Services or Red Hat Enterprise Linux OpenStack Platform.	You do not need to install an agent.
Provision virtual machines by integrating with a vSphere environment.	“Installing and Configuring the Proxy Agent for vSphere,” on page 99
Provision virtual machines by integrating with a Microsoft Hyper-V Server environment.	“Installing the Proxy Agent for Hyper-V or XenServer,” on page 104
Provision virtual machines by integrating with a XenServer environment.	<ul style="list-style-type: none"> ■ “Installing the Proxy Agent for Hyper-V or XenServer,” on page 104 ■ “Installing the EPI Agent for Citrix,” on page 111
Provision virtual machines by integrating with a XenDesktop environment.	<ul style="list-style-type: none"> ■ “Installing the VDI Agent for XenDesktop,” on page 108 ■ “Installing the EPI Agent for Citrix,” on page 111

Table 4-13. Choosing an Agent Scenario (Continued)

Integration Scenario	Agent Requirements and Procedures
Run Visual Basic scripts as additional steps in the provisioning process before or after provisioning a machine, or when deprovisioning.	“Installing the EPI Agent for Visual Basic Scripting,” on page 114
Collect data from the provisioned Windows machines, for example the Active Directory status of the owner of a machine.	“Installing the WMI Agent for Remote WMI Requests,” on page 117
Provision virtual machines by integrating with any other supported virtual platform.	You do not need to install an agent.

Agent Installation Location and Requirements

A system administrator typically installs the agents on the vRealize Automation server that hosts the active Manager Service component.

If an agent is installed on another host, the network configuration must allow communication between the agent and Manager Services installation machine.

Each agent is installed under a unique name in its own directory, `Agents\agentname`, under the vRealize Automation installation directory (typically `Program Files(x86)\VMware\vCAC`), with its configuration stored in the file `VRMAgent.exe.config` in that directory.

Installing and Configuring the Proxy Agent for vSphere

A system administrator installs proxy agents to communicate with vSphere server instances. The agents discover available work, retrieve host information, and report completed work items and other host status changes.

vSphere Agent Requirements

vSphere endpoint credentials, or the credentials under which the agent service runs, must have administrative access to the installation host. Multiple vSphere agents must meet vRealize Automation configuration requirements.

Credentials

When creating an endpoint representing the vCenter Server instance to be managed by a vSphere agent, the agent can use the credentials that the service is running under to interact with the vCenter Server or specify separate endpoint credentials.

The following table lists the permissions that the vSphere endpoint credentials must have to manage a vCenter Server instance. The permissions must be enabled for all clusters in vCenter Server, not just clusters that will host endpoints.

Table 4-14. Permissions Required for vSphere Agent to Manage vCenter Server Instance

Attribute Value	Permission
Datastore	Allocate Space
	Browse Datastore
Datastore Cluster	Configure a Datastore Cluster
Folder	Create Folder
	Delete Folder
Global	Manage Custom Attributes
	Set Custom Attribute

Table 4-14. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

Attribute Value		Permission
Network		Assign Network
Permissions		Modify Permission
Resource		Assign VM to Res Pool
		Migrate Powered Off Virtual Machine
		Migrate Powered On Virtual Machine
Virtual Machine	Inventory	Create from existing
		Create New
		Move
		Remove
	Interaction	Configure CD Media
		Console Interaction
		Device Connection
		Power Off
		Power On
		Reset
		Suspend
		Tools Install
		Configuration
	Add New Disk	
	Add or Remove Device	
	Remove Disk	
	Advanced	
	Change CPU Count	
	Change Resource	
	Extend Virtual Disk	
	Disk Change Tracking	
	Memory	
	Modify Device Settings	
	Rename	
	Set Annotation (version 5.0 and later)	
	Settings	
	Swapfile Placement	
	Provisioning	Customize
		Clone Template
		Clone Virtual Machine
		Deploy Template
		Read Customization Specs
	State	Create Snapshot

Table 4-14. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

Attribute Value	Permission
	Remove Snapshot
	Revert to Snapshot

Disable or reconfigure any third-party software that might change the power state of virtual machines outside of vRealize Automation. Such changes can interfere with the management of the machine life cycle by vRealize Automation.

Install the vSphere Agent

Install a vSphere agent to manage vCenter Server instances. For high availability, you can install a second, redundant vSphere agent for the same vCenter Server instance. You must name and configure both vSphere agents identically, and install them on different machines.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have completed all the “[vSphere Agent Requirements](#),” on page 99.
- If you already created a vSphere endpoint for use with this agent, make a note of the endpoint name.
- “[Download the vRealize Automation IaaS Installer](#),” on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Custom Install** on the Installation Type page.
- 6 In the Component Selection area, select **Proxy Agents**.
- 7 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 8 Click **Next**.

- 9 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.

- 10 Click **Next**.

- 11 Select vSphere from the **Agent type** list.

- 12 Enter an identifier for this agent in the **Agent name** text box.

Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 13 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 14 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Click **Test** to verify connectivity to each host.

- 16 Enter the name of the endpoint.

The endpoint name that you configure in vRealize Automation must match the endpoint name provided to the vSphere proxy agent during installation or the endpoint cannot function.

- 17 Click **Add**.

- 18 Click **Next**.

- 19 Click **Install** to begin the installation.

After several minutes a success message appears.

- 20 Click **Next**.
- 21 Click **Finish**.
- 22 Verify that the installation is successful.
- 23 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

[“Configure the vSphere Agent,”](#) on page 103.

Configure the vSphere Agent

Configure the vSphere agent in preparation for creating and using vSphere endpoints within vRealize Automation blueprints.

You use the proxy agent utility to modify encrypted portions of the agent configuration file, or to change the machine deletion policy for virtualization platforms. Only part of the `VRMAgent.exe.config` agent configuration file is encrypted. For example, the `serviceConfiguration` section is unencrypted.

Prerequisites

Using an account with administrator privileges, log in to the IaaS Windows server where you installed the vSphere agent.

Procedure

- 1 Open a Windows command prompt as an administrator.
- 2 Change to the agent installation folder, where *agent-name* is the folder containing the vSphere agent.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\agent-name
```

- 3 (Optional) To view the current configuration settings, enter the following command.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

The following is an example of the command output.

```
managementEndpointName: VCEndpoint
doDeletes: True
```

- 4 (Optional) To change the name of the endpoint that you configured at installation, use the following command.

```
set managementEndpointName
```

For example: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

You use this process to rename the endpoint within vRealize Automation, instead of changing endpoints.

- 5 (Optional) To configure the virtual machine deletion policy, use the following command.

```
set doDeletes
```

For example: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

Option	Description
true	(Default) Delete virtual machines destroyed in vRealize Automation from vCenter Server.
false	Move virtual machines destroyed in vRealize Automation to the <code>VRMDeleted</code> directory in vCenter Server.

- 6 (Optional) To require a trusted certificate for the vSphere agent, modify `VRMAgent.exe.config` in a text editor.

In the `serviceConfiguration` section, set the `trustAllCertificates` parameter to `false`.

```
trustAllCertificates = "false"
```

Because the setting is unencrypted, you do not use a `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set trustAllCertificates false` command.

Option	Description
true	(Default) The vSphere agent does not require a trusted certificate from vCenter Server.
false	The vSphere agent requires a trusted certificate from vCenter Server.

- 7 Open **Administrative Tools > Services** and restart the vRealize Automation Agent – *agent-name* service.

What to do next

For high-availability, you can install and configure a redundant agent for your endpoint. Install each redundant agent on a separate server, but name and configure the agents identically.

Installing the Proxy Agent for Hyper-V or XenServer

A system administrator installs proxy agents to communicate with Hyper-V and XenServer server instances. The agents discover available work, retrieve host information, and report completed work items and other host status changes.

Hyper-V and XenServer Requirements

Hyper-V Hypervisor proxy agents require system administrator credentials for installation.

The credentials under which to run the agent service must have administrative access to the installation host.

Administrator-level credentials are required for all XenServer or Hyper-V instances on the hosts to be managed by the agent.

If you are using Xen pools, all nodes within the Xen pool must be identified by their fully qualified domain names.

NOTE By default, Hyper-V is not configured for remote management. A vRealize Automation Hyper-V proxy agent cannot communicate with a Hyper-V server unless remote management has been enabled.

See the Microsoft Windows Server documentation for information about how to configure Hyper-V for remote management.

Install the Hyper-V or XenServer Agent

The Hyper-V agent manages Hyper-V server instances. The XenServer agent manages XenServer server instances.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.
- Verify that Hyper-V Hypervisor proxy agents have system administrator credentials.
- Verify that the credentials under which to run the agent service have administrative access to the installation host.

- Verify that all XenServer or Hyper-V instances on the hosts to be managed by the agent have administrator-level credentials.
- If you are using Xen pools, note that all nodes within the Xen pool must be identified by their fully qualified domain names.
vRealize Automation cannot communicate with or manage any node that is not identified by its fully qualified domain name within the Xen pool.
- Configure Hyper-V for remote management to enable Hyper-V server communication with vRealize Automation Hyper-V proxy agents.
See the Microsoft Windows Server documentation for information about how to configure Hyper-V for remote management.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Custom Install** on the Installation Type page.
- 6 Select **Component Selection** on the Installation Type page.
- 7 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 8 Click **Next**.
- 9 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.
- 10 Click **Next**.
- 11 Select the agent from the **Agent type** list.
 - Xen
 - Hyper-V

- 12 Enter an identifier for this agent in the **Agent name** text box.

Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 13 Communicate the **Agent name** to the IaaS administrator who configures endpoints.
To enable access and data collection, the endpoint must be linked to the agent that was configured for it.
- 14 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 16 Click **Test** to verify connectivity to each host.
- 17 Enter the credentials of a user with administrative-level permissions on the managed server instance.
- 18 Click **Add**.
- 19 Click **Next**.
- 20 (Optional) Add another agent.
For example, you can add a Xen agent if you previously added the Hyper-V agent.
- 21 Click **Install** to begin the installation.
After several minutes a success message appears.
- 22 Click **Next**.

- 23 Click **Finish**.
- 24 Verify that the installation is successful.

What to do next

For high-availability, you can install and configure a redundant agent for your endpoint. Install each redundant agent on a separate server, but name and configure the agents identically.

[“Configure the Hyper-V or XenServer Agent,”](#) on page 107.

Configure the Hyper-V or XenServer Agent

A system administrator can modify proxy agent configuration settings, such as the deletion policy for virtualization platforms. You can use the proxy agent utility to modify the initial configurations that are encrypted in the agent configuration file.

Prerequisites

Log in as a **system administrator** to the machine where you installed the agent.

Procedure

- 1 Change to the agents installation directory, where *agent_name* is the directory containing the proxy agent, which is also the name under which the agent is installed.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2 View the current configuration settings.

```
Enter DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

The following is an example of the output of the command:

```
Username: XSAdmin
```

- 3 Enter the set command to change a property, where *property* is one of the options shown in the table.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set property value
```

If you omit *value*, the utility prompts you for a new value.

Property	Description
username	The username representing administrator-level credentials for the XenServer or Hyper-V server the agent communicates with.
password	The password for the administrator-level username.

- 4 Click **Start > Administrative Tools > Services** and restart the vRealize Automation Agent – *agentname* service.

Example: Change Administrator-Level Credentials

Enter the following command to change the administrator-level credentials for the virtualization platform specified during the agent installation.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

What to do next

For high-availability, you can install and configure a redundant agent for your endpoint. Install each redundant agent on a separate server, but name and configure the agents identically.

Installing the VDI Agent for XenDesktop

vRealize Automation uses Virtual Desktop Integration (VDI) PowerShell agents to register the XenDesktop machines it provisions with external desktop management systems.

The VDI integration agent provides the owners of registered machines with a direct connection to the XenDesktop Web Interface. You can install a VDI agent as a dedicated agent to interact with a single Desktop Delivery Controller (DDC) or as a general agent that can interact with multiple DDCs.

XenDesktop Requirements

A system administrator installs a Virtual Desktop Infrastructure (VDI) agent to integrate XenDesktop servers into vRealize Automation.

You can install a general VDI agent to interact with multiple servers. If you are installing one dedicated agent per server for load balancing or authorization reasons, you must provide the name of the XenDesktop DDC server when installing the agent. A dedicated agent can handle only registration requests directed to the server specified in its configuration.

Consult the *vRealize Automation Support Matrix* on the VMware Web site for information about supported versions of XenDesktop for XenDesktop DDC servers.

Installation Host and Credentials

The credentials under which the agent runs must have administrative access to all XenDesktop DDC servers with which it interacts.

XenDesktop Requirements

The name given to the XenServer Host on your XenDesktop server must match the UUID of the Xen Pool in XenCenter. See [“Set the XenServer Host Name,”](#) on page 109 for more information.

Each XenDesktop DDC server with which you intend to register machines must be configured in the following way:

- The group/catalog type must be set to **Existing** for use with vRealize Automation.
- The name of a vCenter Server host on a DDC server must match the name of the vCenter Server instance as entered in the vRealize Automation vSphere endpoint, without the domain. The endpoint must be configured with a fully qualified domain name (FQDN), and not with an IP address. For example, if the address in the endpoint is `https://virtual-center27.domain/sdk`, the name of the host on the DDC server must be set to `virtual-center27`.

If your vRealize Automation vSphere endpoint has been configured with an IP address, you must change it to use an FQDN. See *IaaS Configuration* for more information about setting up endpoints.

XenDesktop Agent Host requirements

Citrix XenDesktop SDK must be installed. The SDK for XenDesktop is included on the XenDesktop installation disc.

Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.

MS PowerShell Execution Policy is set to RemoteSigned or Unrestricted. See [“Set the PowerShell Execution Policy to RemoteSigned,”](#) on page 98.

For more information about PowerShell Execution Policy, run `help about_signing` or `help Set-ExecutionPolicy` at the PowerShell command prompt.

Set the XenServer Host Name

In XenDesktop, the name given to the XenServer Host on your XenDesktop server must match the UUID of the Xen Pool in XenCenter. If no XenPool is configured, the name must match the UUID of the XenServer itself.

Procedure

- 1 In Citrix XenCenter, select your XenPool or standalone XenServer and click the **General** tab. Record the UUID.
- 2 When you add your XenServer Pool or standalone host to XenDesktop, type the UUID that was recorded in the previous step as the **Connection** name.

Install the XenDesktop Agent

Virtual desktop integration (VDI) PowerShell agents integrate with external virtual desktop system, such as XenDesktop and Citrix. Use a VDI PowerShell agent to manage the XenDesktop machine.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that your environment meets the [“XenDesktop Requirements,”](#) on page 108.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup_vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Click **Next**.
- 6 Select **Custom Install** on the Installation Type page.
- 7 Select **Proxy Agents** in the Component Selection pane.
- 8 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 9 Click **Next**.

- 10 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.
- 11 Click **Next**.
- 12 Select **VdiPowerShell** from the **Agent type** list.
- 13 Enter an identifier for this agent in the **Agent name** text box.

Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 14 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 16 Click **Test** to verify connectivity to each host.
- 17 Select the **VDI version**.
- 18 Enter the fully qualified domain name of the managed server in the **VDI Server** text box.
- 19 Click **Add**.
- 20 Click **Next**.
- 21 Click **Install** to begin the installation.

After several minutes a success message appears.

- 22 Click **Next**.
- 23 Click **Finish**.
- 24 Verify that the installation is successful.
- 25 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

For high-availability, you can install and configure a redundant agent for your endpoint. Install each redundant agent on a separate server, but name and configure the agents identically.

Installing the EPI Agent for Citrix

External provisioning Integration (EPI) PowerShell agents integrate Citrix external machines into the provisioning process. The EPI agent provides on-demand streaming of the Citrix disk images from which the machines boot and run.

The dedicated EPI agent interacts with a single external provisioning server. You must install one EPI agent for each Citrix provisioning server instance.

Citrix Provisioning Server Requirements

A system administrator uses External Provisioning Infrastructure (EPI) agents to integrate Citrix provisioning servers and to enable the use of Visual Basic scripts in the provisioning process.

Installation Location and Credentials

Install the agent on the PVS host for Citrix Provisioning Services instances. Verify that the installation host meets [“Citrix Agent Host Requirements,”](#) on page 111 before you install the agent.

Although an EPI agent can generally interact with multiple servers, Citrix Provisioning Server requires a dedicated EPI agent. You must install one EPI agent for each Citrix Provisioning Server instance, providing the name of the server hosting it. The credentials under which the agent runs must have administrative access to the Citrix Provisioning Server instance.

Consult the *vRealize Automation Support Matrix* for information about supported versions of Citrix PVS.

Citrix Agent Host Requirements

PowerShell and Citrix Provisioning Services SDK must be installed on the installation host prior to agent installation. Consult the *vRealize Automation Support Matrix* on the VMware Web site for details.

Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.

You must also ensure that the PowerShell Snap-In is installed. For more information, see the *Citrix Provisioning Services PowerShell Programmer’s Guide* on the Citrix Web site.

MS PowerShell Execution Policy is set to RemoteSigned or Unrestricted. See [“Set the PowerShell Execution Policy to RemoteSigned,”](#) on page 98.

For more information about PowerShell Execution Policy, run `help about_signing` or `help Set-ExecutionPolicy` at the PowerShell command prompt.

Install the Citrix Agent

External provisioning integration (EPI) PowerShell agents integrate external systems into the machine provisioning process. Use the EPI PowerShell agent to integrate with Citrix provisioning server to enable provisioning of machines by on-demand disk streaming.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the [“Citrix Provisioning Server Requirements,”](#) on page 111.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Custom Install** on the Installation Type page.
- 6 Select **Component Selection** on the Installation Type page.
- 7 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 8 Click **Next**.
- 9 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.
- 10 Click **Next**.
- 11 Select **EPIPowerShell** from the Agent type list.

- 12 Enter an identifier for this agent in the **Agent name** text box.

Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 13 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 14 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Click **Test** to verify connectivity to each host.
- 16 Select the EPI type.
- 17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.
- 18 Click **Add**.
- 19 Click **Next**.
- 20 Click **Install** to begin the installation.
After several minutes a success message appears.
- 21 Click **Next**.
- 22 Click **Finish**.
- 23 Verify that the installation is successful.
- 24 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

For high-availability, you can install and configure a redundant agent for your endpoint. Install each redundant agent on a separate server, but name and configure the agents identically.

Installing the EPI Agent for Visual Basic Scripting

A system administrator can specify Visual Basic scripts as additional steps in the provisioning process before or after provisioning a machine, or when deprovisioning a machine. You must install an External Provisioning Integration (EPI) PowerShell before you can run Visual Basic scripts.

Visual Basic scripts are specified in the blueprint from which machines are provisioned. Such scripts have access to all of the custom properties associated with the machine and can update their values. The next step in the workflow then has access to these new values.

For example, you could use a script to generate certificates or security tokens before provisioning and use them in machine provisioning.

To enable scripts in provisioning, you must install a specific type of EPI agent and place the scripts you want to use on the system on which the agent is installed.

When executing a script, the EPI agent passes all machine custom properties as arguments to the script. To return updated property values, you must place these properties in a dictionary and call a vRealize Automation function. A sample script is included in the scripts subdirectory of the EPI agent installation directory. This script contains a header to load all arguments into a dictionary, a body in which you can include your function(s), and a footer to return updated custom properties values.

NOTE You can install multiple EPI/VBScripts agents on multiple servers and provision using a specific agent and the Visual Basic scripts on that agent's host. If you need to do this, contact VMware customer support.

Visual Basic Scripting Requirements

A system administrator installs External Provisioning Infrastructure (EPI) agents to enable the use of Visual Basic scripts in the provisioning process.

The following table describes the requirements that apply to installing an EPI agent to enable the use of Visual Basic scripts in the provisioning process.

Table 4-15. EPI Agents for Visual Scripting

Requirement	Description
Credentials	Credentials under which the agent will run must have administrative access to the installation host.
Microsoft PowerShell	Microsoft PowerShell must be installed on the installation host prior to agent installation: The version required depends on the operating system of the installation host and might have been installed with that operating system. Visit http://support.microsoft.com for more information.
MS PowerShell Execution Policy	MS PowerShell Execution Policy must be set to RemoteSigned or Unrestricted . For information on PowerShell Execution Policy issue one of the following commands at Power-Shell command prompt: <pre>help about_signing help Set-ExecutionPolicy</pre>

Install the Agent for Visual Basic Scripting

External provisioning integration (EPI) PowerShell agents allow integrate external systems into the machine provisioning process. Use an EPI agent to run Visual Basic Scripts as extra steps during the provisioning process.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the [“Visual Basic Scripting Requirements,”](#) on page 114.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Custom Install** on the Installation Type page.
- 6 Select **Component Selection** on the Installation Type page.
- 7 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 8 Click **Next**.
- 9 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.
- 10 Click **Next**.
- 11 Select **EPIPowerShell** from the Agent type list.

- 12 Enter an identifier for this agent in the **Agent name** text box.

Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 13 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 14 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Click **Test** to verify connectivity to each host.
- 16 Select the EPI type.
- 17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.
- 18 Click **Add**.
- 19 Click **Next**.
- 20 Click **Install** to begin the installation.
After several minutes a success message appears.
- 21 Click **Next**.
- 22 Click **Finish**.
- 23 Verify that the installation is successful.
- 24 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

Installing the WMI Agent for Remote WMI Requests

A system administrator enables the Windows Management Instrumentation (WMI) protocol and installs the WMI agent on all managed Windows machines to enable management of data and operations. The agent is required to collect data from Windows machines, such as the Active Directory status of the owner of a machine.

Enable Remote WMI Requests on Windows Machines

To use WMI agents, remote WMI requests must be enabled on the managed Windows servers.

Procedure

- 1 In each domain that contains provisioned and managed Windows virtual machines, create an Active Directory group and add to it the service credentials of the WMI agents that execute remote WMI requests on the provisioned machines.
- 2 Enable remote WMI requests for the Active Directory groups containing the agent credentials on each Windows machine provisioned.

Install the WMI Agent

The Windows Management Instrumentation (WMI) agent enables data collection from Windows managed machines.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the requirements, see [“Enable Remote WMI Requests on Windows Machines,”](#) on page 117.
- [“Download the vRealize Automation IaaS Installer,”](#) on page 76.

Procedure

- 1 Right-click the `setup__vrealize-automation-appliance-FQDN@5480.exe` setup file and select **Run as administrator**.
- 2 Click **Next**.
- 3 Accept the license agreement and click **Next**.
- 4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
 - a Type the user name, which is **root**, and the password.
The password is the password that you specified when you deployed the vRealize Automation appliance.
 - b Select **Accept Certificate**.
 - c Click **View Certificate**.
Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
- 5 Select **Custom Install** on the Installation Type page.
- 6 Select **Component Selection** on the Installation Type page.

- 7 Accept the root install location or click **Change** and select an installation path.
Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
If you install more than one IaaS component, always install them to the same path.
- 8 Click **Next**.
- 9 Log in with administrator privileges for the Windows services on the installation machine.
The service must run on the same installation machine.
- 10 Click **Next**.
- 11 Select **WMI** from the **Agent type** list.
- 12 Enter an identifier for this agent in the **Agent name** text box.
Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

IMPORTANT For high availability, you may add redundant agents and configure them identically. Otherwise, keep agents unique.

Option	Description
Redundant agent	Install redundant agents on different servers. Name and configure redundant agents identically.
Standalone agent	Assign a unique name to the agent.

- 13 Configure a connection to the IaaS Manager Service host.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, <i>mgr-svc.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 14 Configure a connection to the IaaS Web server.

Option	Description
With a load balancer	Enter the fully qualified domain name and port number of the load balancer for the Web server component, <i>web-load-balancer.mycompany.com:443</i> . Do not enter IP addresses.
Without a load balancer	Enter the fully qualified domain name and port number of the machine where you installed the Web server component, <i>web.mycompany.com:443</i> . Do not enter IP addresses.

The default port is 443.

- 15 Click **Test** to verify connectivity to each host.
- 16 Click **Add**.
- 17 Click **Next**.

- 18 Click **Install** to begin the installation.
After several minutes a success message appears.
- 19 Click **Next**.
- 20 Click **Finish**.
- 21 Verify that the installation is successful.
- 22 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

vRealize Automation Post-Installation Tasks

5

After you install vRealize Automation, there are post-installation tasks that might need your attention.

This chapter includes the following topics:

- [“Configure Federal Information Processing Standard Compliant Encryption,”](#) on page 121
- [“Replacing Self-Signed Certificates with Certificates Provided by an Authority,”](#) on page 122
- [“Change the Master vRealize Automation Appliance Host Name,”](#) on page 122
- [“Change a Replica vRealize Automation Appliance Host Name,”](#) on page 123
- [“Installing the vRealize Log Insight Agent on IaaS Servers,”](#) on page 124
- [“Configure Access to the Default Tenant,”](#) on page 124

Configure Federal Information Processing Standard Compliant Encryption

You can enable or disable Federal Information Processing Standard (FIPS) 140–2 compliant cryptography for inbound and outbound vRealize Automation appliance network traffic.

Changing the FIPS setting requires a vRealize Automation restart. FIPS is disabled by default.

Procedure

- 1 Log in as root to the vRealize Automation appliance management interface.

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

- 2 Click **vRA Settings > Host Settings**.
- 3 Near the upper right, click the button to enable or disable FIPS.

When enabled, inbound and outbound vRealize Automation appliance network traffic on port 443 uses FIPS 140–2 compliant encryption. Regardless of the FIPS setting, vRealize Automation uses AES–256 compliant algorithms to protect secured data stored on the vRealize Automation appliance.

NOTE This vRealize Automation release only partially enables FIPS compliance, because some internal components do not yet use certified cryptographic modules. In cases where certified modules have not yet been implemented, the AES–256 compliant algorithms are used.

- 4 Click **Yes** to restart vRealize Automation.

You can also configure FIPS from a vRealize Automation appliance console session as root, using the following commands.

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

Replacing Self-Signed Certificates with Certificates Provided by an Authority

If you installed vRealize Automation with self-signed certificates, you might want to replace them with certificates provided by a certificate authority before deploying to production.

For more information about updating certificates, see *Managing vRealize Automation*.

Change the Master vRealize Automation Appliance Host Name

When maintaining an environment or network, you might need to assign a different host name to an existing master vRealize Automation appliance.

In a high availability cluster of vRealize Automation appliances, follow these steps to change the host name of the primary, or master, vRealize Automation appliance node.

Procedure

- 1 In DNS, create an additional record with the new master host name.
Do not remove the existing DNS record with the old host name yet.
- 2 Wait for DNS replication and zone distribution to occur.
- 3 From a console session as root on the master vRealize Automation appliance, run the following script.
`/usr/lib/vcac/tools/change-hostname/changeHostName-master.sh new-master-hostname`
- 4 Log in as root to the master vRealize Automation appliance management interface.
`https://vrealize-automation-appliance-FQDN:5480`
- 5 Click **Network > Address**.
- 6 In the **Hostname** text box, enter the new master host name, and click **Save Settings**.
- 7 From a console session as root, update the HAProxy configuration with the new master host name.
On all vRealize Automation appliances in the cluster, including master and replicas, use a text editor to replace the old master host name throughout the files in the following directory.
`/etc/haproxy/conf.d`
- 8 Restart the master vRealize Automation appliance.
- 9 Restart replica vRealize Automation appliances, one at a time.
- 10 Log in as root to the master vRealize Automation appliance management interface.
- 11 Click **vRA Settings > Database**.
- 12 Reset any replica nodes that show a Status of N/A.
- 13 Verify that the Sync State is correct for database replication on each vRealize Automation appliance node.
- 14 Click **vRA Settings > Cluster**.
- 15 Use **Join Cluster** to re-join each replica node to the cluster.

- 16 Restart each replica node.
- 17 In DNS, remove the existing DNS record with the old master host name.

Change a Replica vRealize Automation Appliance Host Name

When maintaining an environment or network, you might need to assign a different host name to an existing replica vRealize Automation appliance.

In a high availability cluster of vRealize Automation appliances, follow these steps to change the host name of a replica vRealize Automation appliance node.

Prerequisites

If the master node host name needs to change, complete that entire procedure first. See [“Change the Master vRealize Automation Appliance Host Name,”](#) on page 122.

Procedure

- 1 In DNS, create an additional record with the new replica host name.
Do not remove the existing DNS record with the old host name yet.
- 2 Wait for DNS replication and zone distribution to occur.
- 3 From a console session as root on the replica vRealize Automation appliance, run the following script.
`/usr/lib/vcac/tools/change-hostname/changeHostName-replica.sh new-replica-hostname`
- 4 From a console session as root on the master vRealize Automation appliance, run the following script.
`changeHostName-master.sh new-replica-hostname old-replica-hostname`
- 5 Log in as root to the replica vRealize Automation appliance management interface.
`https://vrealize-automation-appliance-FQDN:5480`
- 6 Click **Network > Address**.
- 7 In the **Hostname** text box, enter the new replica host name, and click **Save Settings**.
- 8 From a console session as root, update the HAProxy configuration with the new replica host name.
On all vRealize Automation appliances in the cluster, including master and replicas, use a text editor to replace the old replica host name throughout the files in the following directory.
`/etc/haproxy/conf.d`
- 9 Restart the master vRealize Automation appliance.
- 10 Restart replica vRealize Automation appliances, one at a time.
- 11 Log in as root to the master vRealize Automation appliance management interface.
- 12 Click **vRA Settings > Database**.
- 13 Reset any replica nodes that show a Status of N/A.
- 14 Verify that the Sync State is correct for database replication on each vRealize Automation appliance node.
- 15 Click **vRA Settings > Cluster**.
- 16 Use **Join Cluster** to re-join each replica node to the cluster.

- 17 Restart each replica node.

NOTE Afterward, RabbitMQ might still show the old replica node being in the cluster, but the old host name is shown as Not Connected and is safe to ignore.

- 18 In DNS, remove the existing DNS record with the old replica host name.

Installing the vRealize Log Insight Agent on IaaS Servers

The Windows servers in a vRealize Automation IaaS configuration do not include the vRealize Log Insight agent by default.

vRealize Log Insight provides log aggregation and indexing, and can collect, import, and analyze logs to expose system problems. If you want to capture and analyze logs from IaaS servers by using vRealize Log Insight, you must separately install the vRealize Log Insight agent for Windows. See the *VMware vRealize Log Insight Agent Administration Guide*.

vRealize Automation appliances include the vRealize Log Insight agent by default.

Configure Access to the Default Tenant

You must grant your team access rights to the default tenant before they can begin configuring vRealize Automation.

The default tenant is automatically created when you configure single sign-on in the installation wizard. You cannot edit the tenant details, such as the name or URL token, but you can create new local users and appoint additional tenant or IaaS administrators at any time.

Procedure

- 1 Log in to vRealize Automation as the administrator of the default tenant.
 - a Navigate to the vRealize Automation product interface.
`https://vrealize-automation-FQDN/vcac`
 - b Log in with the user name **administrator** and the password you defined for this user when you configured SSO.
- 2 Select **Administration > Tenants**.
- 3 Click the name of the default tenant, **vsphere.local**.
- 4 Click the **Local users** tab.
- 5 Create local user accounts for the vRealize Automation default tenant.
Local users are tenant-specific and can only access the tenant in which you created them.
 - a Click the Add (+) icon.
 - b Enter details for the user responsible for administering your infrastructure.
 - c Click **Add**.
 - d Repeat this step to add one or more additional users who are responsible for configuring the default tenant.
- 6 Click the **Administrators** tab.

- 7 Assign your local users to the tenant administrator and IaaS administrator roles.
 - a Enter a username in the **Tenant administrators** search box and press Enter.
 - b Enter a username in the **IaaS administrators** search box and press Enter.

The IaaS administrator is responsible for creating and managing your infrastructure endpoints in vRealize Automation. Only the system administrator can grant this role.

- 8 Click **Update**.

What to do next

Provide your team with the access URL and log in information for the user accounts you created so they can begin configuring vRealize Automation.

- Your tenant administrators configure settings such as user authentication, including configuring Directories Management for high availability. See *Configuring vRealize Automation*.
- Your IaaS administrators prepare external resources for provisioning. See *Configuring vRealize Automation*.
- If you configured Initial Content Creation during the installation, your configuration administrator can request the Initial Content catalog item to quickly populate a proof of concept. For an example of how to request the item and complete the manual user action, see *Installing and Configuring vRealize Automation for the Rainpole Scenario*.

Troubleshooting a vRealize Automation Installation

6

vRealize Automation troubleshooting provides procedures for resolving issues you might encounter when installing or configuring vRealize Automation.

This chapter includes the following topics:

- [“Default Log Locations,”](#) on page 127
- [“Rolling Back a Failed Installation,”](#) on page 128
- [“Create a vRealize Automation Support Bundle,”](#) on page 130
- [“General Installation Troubleshooting,”](#) on page 130
- [“Troubleshooting the vRealize Automation Appliance,”](#) on page 134
- [“Troubleshooting IaaS Components,”](#) on page 138
- [“Troubleshooting Log-In Errors,”](#) on page 144

Default Log Locations

Consult system and product log files for information on a failed installation.

NOTE For log collection, consider taking advantage of the vRealize Automation and vRealize Orchestrator Content Packs for vRealize Log Insight. The Content Packs and Log Insight provide a consolidated summary of log events for components in the vRealize suite. For more information, visit the [VMware Solution Exchange](#).

For the most recent log location list, see [VMware Knowledge Base article 2141175](#).

Windows Logs

Use the following to find log files for Windows events.

Log	Location
Windows Event Viewer logs	Start > Control Panel > Administrative Tools > Event Viewer

Installation Logs

Installation logs are in the following locations.

Log	Default Location
Installation Logs	C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log
WAPI Installation Logs	C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

IaaS Logs

IaaS logs are in the following locations.

Log	Default Location
Website Logs	C:\Program Files (x86)\VMware\vCAC\Server\Website\Log
Repository Log	C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Log
Manager Service Logs	C:\Program Files (x86)\VMware\vCAC\Server\Log
DEM Orchestrator Logs	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Log
Agent Logs	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\log

vRealize Automation Framework Logs

Log entries for vRealize Automation Frameworks are located in the following location.

Log	Default location
Framework Logs	/var/log/vmware

Software Component Provisioning Logs

Software component provisioning logs are located in the following location.

Log	Default Location
Software Agent Bootstrap Log	/opt/vmware-appdirector (for Linux) or \opt\vmware-appdirector (for Windows)
Software Lifecycle Script Logs	/tmp/taskId (for Linux) \Users\darwin\AppData\Local\Temp\taskId (for Windows)

Collection of Logs for Distributed Deployments

You can create a zip file that bundles all logs for components of a distributed deployment. .

Rolling Back a Failed Installation

When an installation fails and rolls back, the system administrator must verify that all required files have been uninstalled before starting another installation. Some files must be uninstalled manually.

Roll Back a Minimal Installation

A system administrator must manually remove some files and revert the database to completely uninstall a failed vRealize Automation IaaS installation.

Procedure

- 1 If the following components are present, uninstall them with the Windows uninstaller.
 - vRealize Automation Agents
 - vRealize Automation DEM-Worker
 - vRealize Automation DEM-Orchestrator
 - vRealize Automation Server
 - vRealize Automation WAPI

NOTE If you see the following message, restart the machine and then follow the steps in this procedure: Error opening installation log file. Verify that the specified log file location exists and it is writable

NOTE If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.

- 2 Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.
- 3 In IIS (Internet Information Services Manager) select Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).
- 4 Check that the Applications Repository, vRealize Automation and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.

The installation is completely removed.

Roll Back a Distributed Installation

A system administrator must manually remove some files and revert the database to completely uninstall a failed IaaS installation.

Procedure

- 1 If the following components are present, uninstall them with the Windows uninstaller.
 - vRealize Automation Server
 - vRealize Automation WAPI

NOTE If you see the following message, restart the machine and then follow this procedure: Error opening installation log file. Verify that the specified log file location exists and it is writable.

NOTE If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.

- 2 Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.
- 3 In IIS (Internet Information Services Manager) select the Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).
- 4 Check that the Applications Repository, vCAC and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.

Table 6-1. Roll Back Failure Points

Failure Point	Action
Installing Manager Service	If present, uninstall vCloud Automation Center Server.
Installing DEM-Orchestrator	If present, uninstall the DEM Orchestrator .
Installing DEM-Worker	If present, uninstall all DEM Workers
Installing an Agent	If present, uninstall all vRealize Automation agents.

Create a vRealize Automation Support Bundle

You can create a vRealize Automation support bundle using the vRealize Automation appliance management interface. Support bundles gather logs, and help you or VMware technical support to troubleshoot vRealize Automation problems.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Log in as root, and click **vRA Settings > Cluster**.
- 3 Click **Create Support Bundle**.
- 4 Click **Download** and save the support bundle file on your system.

Support bundles include information from the vRealize Automation appliance and IaaS Windows servers. If you lose connectivity between the vRealize Automation appliance and IaaS components, the support bundle might be missing the IaaS component logs.

To see which log files were collected, unzip the support bundle and open the `Environment.html` file in a Web browser. Without connectivity, IaaS components might appear in red in the Nodes table. Another reason that the IaaS logs are missing might be that the vRealize Automation Management Agent service has stopped on IaaS Windows servers that appear in red.

For a back-up procedure to collect IaaS component log bundles, see [VMware Knowledge Base article 2078179](#).

General Installation Troubleshooting

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Installation or Upgrade Fails with a Load Balancer Timeout Error

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

Problem

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.

Cause

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

Solution

- 1 Increase your load balancer timeout value to at least 100 seconds. For example, and depending on the load balancer you are using, edit the load balancer timeout setting in your `ssl.conf`, `httpd.conf` or other Web configuration file.
- 2 Rerun the installation or upgrade.

Server Times Are Not Synchronized

An installation might not succeed when IaaS time servers are not synchronized with the vRealize Automation appliance.

Problem

You cannot log in after installation, or the installation fails while it is completing.

Cause

Time servers on all servers might not be synchronized.

Solution

For each vRealize Automation appliance server and all Windows servers where the IaaS components will be installed, enable time synchronization as described in the following topics:

- [“Enable Time Synchronization on the vRealize Automation Appliance,”](#) on page 52
- [“Enable Time Synchronization on the Windows Server,”](#) on page 55

For an overview of timekeeping for vRealize Automation, see [“Time Synchronization,”](#) on page 31.

Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7

When you use Internet Explorer 9 or 10 on Windows 7 and compatibility mode is enabled, some pages appear to have no content.

Problem

When using Internet Explorer 9 or 10 on Windows 7, the following pages have no content:

- Infrastructure
- Default Tenant Folder on the Orchestrator page
- Server Configuration on the Orchestrator page

Cause

The problem could be related to compatibility mode being enabled. You can disable compatibility mode for Internet Explorer with the following steps.

Solution**Prerequisites**

Ensure that the menu bar is displayed. If you are using Internet Explorer 9 or 10, press Alt to display the Menu bar (or right-click the Address bar and then select **Menu bar**).

Procedure

- 1 Select **Tools > Compatibility View settings**.
- 2 Deselect **Display intranet sites in Compatibility View**.
- 3 Click **Close**.

Cannot Establish Trust Relationship for the SSL/TLS Secure Channel

You might receive the message "Cannot establish trust relationship for the SSL/TLS secure channel when upgrading security certificates for vCloud Automation Center."

Problem

If a certificate issue occurs with `vcac-config.exe` when upgrading a security certificate, you might see the following message:

The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel

You can find more information about the cause of the issue by using the following procedure.

Solution

- 1 Open `vcac-config.exe.config` in a text editor, and locate the repository address:

```
<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />
```
- 2 Open Internet Explorer to the address.
- 3 Continue through any error messages about certificate trust issues.
- 4 Obtain a security report from Internet Explorer, and use it to troubleshoot why the certificate is not trusted.

If problems persist, repeat the procedure by browsing with the address that needs to be registered, the Endpoint address that you used to register with `vcac-config.exe`.

Connect to the Network Through a Proxy Server

Some sites might connect to the Internet through a proxy server.

Problem

Your deployment cannot connect to the open Internet. For example, you cannot access Web sites, public clouds that you manage, or vendor addresses from which you download software or updates.

Cause

Your site connects to the Internet through a proxy server.

Solution

Prerequisites

Obtain proxy server names, port numbers, and credentials from the administrator for your site.

Procedure

- 1 Open a Web browser to the vRealize Automation appliance management interface URL.

```
https://vrealize-automation-appliance-FQDN:5480
```
- 2 Log in as root, and click **Network**.
- 3 Enter your site proxy server FQDN or IP address, and port number.
- 4 If your proxy server requires credentials, enter the user name and password.
- 5 Click **Save Settings**.

What to do next

Configuring to use a proxy might affect VMware Identity Manager user access. To correct the issue, see [“Proxy Prevents VMware Identity Manager User Log In,”](#) on page 145.

Console Steps for Initial Content Configuration

There is an alternative to using the vRealize Automation installation interface to create the configuration administrator account and initial content.

Problem

As the last part of installing vRealize Automation, you follow the process to enter a new password, create the configurationadmin local user account, and create initial content. An error occurs, and the interface enters an unrecoverable state.

Solution

Instead of using the interface, enter console commands to create the configurationadmin user and initial content. Note that the interface might fail after successfully completing part of the process, so you might only need some of the commands.

For example, you might inspect logs and vRealize Orchestrator workflow execution, and determine that the interface-based setup created the configurationadmin user but not the initial content. In that case, you can enter just the last two console commands to complete the process.

Procedure

- 1 Log in to the vRealize Automation appliance console as root.
- 2 Import the vRealize Orchestrator workflow by entering the following command:

```
/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 Execute the workflow to create the configurationadmin user:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.p
y --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --
configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 Import the ASD blueprint by entering the following command:

```
/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 Execute the workflow to configure initial content:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.p
y --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --
configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

Cannot Downgrade vRealize Automation Licenses

An error occurs when you submit the license key of a lower product edition.

Problem

You see the following message when using the vRealize Automation administration interface Licensing page to submit the key to a product edition that is lower than the current one. For example, you start with an enterprise license and try to enter an advanced license.

Unable to downgrade existing license edition

Cause

This vRealize Automation release does not support the downgrading of licenses. You can only add licenses of an equal or higher edition.

Solution

To change to a lower edition, reinstall vRealize Automation.

Troubleshooting the vRealize Automation Appliance

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using your vRealize Automation appliances.

Installers Fail to Download

Installers fail to download from the vRealize Automation appliance.

Problem

Installers do not download when running `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Cause

- Network connectivity issues when connecting to the vRealize Automation appliance machine.
- Not able to connect to the vRealize Automation appliance machine because the machine cannot be reached or it cannot respond before the connection times out.

Solution

- 1 Verify that you can connect to the vRealize Automation URL in a Web browser.
`https://vrealize-automation-appliance-FQDN`
- 2 Check the other vRealize Automation appliance troubleshooting topics.
- 3 Download the setup file and reconnect to the vRealize Automation appliance.

Encryption.key File has Incorrect Permissions

A system error can result when incorrect permissions are assigned to the Encryption.key file for a virtual appliance.

Problem

You log in to vRealize Automation appliance and the Tenants page is displayed. After the page has begun loading, you see the message System Error.

Cause

The Encryption.key file has incorrect permissions or the group or owner user level is incorrectly assigned.

Solution**Prerequisites**

Log in to the virtual appliance that displays the error.

NOTE If your virtual appliances are running under a load balancer, you must check each virtual appliance.

Procedure

- 1 View the log file `/var/log/vcac/catalina.out` and search for the message `Cannot write to /etc/vcac/Encryption.key`.
- 2 Go to the `/etc/vcac/` directory and check the permissions and ownership for the `Encryption.key` file. You should see a line similar to the following one:

```
--rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Read and write permission is required and the owner and group for the file must be `vcac`.

- 3 If the output you see is different, change the permissions or ownership of the file as needed.

What to do next

Log in to the Tenant page to verify that you can log in without error.

Identity Manager Fails to Start After Horizon-Workspace Restart

In a vRealize Automation high availability environment, the Identity Manager can fail to start after the horizon-workspace service is restarted.

Problem

The horizon-workspace service cannot start due an error similar to the following:

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Cause

The Identity Manager may fail to start in a high availability environment due to issues with the liquibase data management utility used by vRealize Automation.

Solution

- 1 Log in to the vRealize Automation appliance as root using `ssh`.
- 2 Run the `service horizon-workspace stop` command to stop the horizon-workspace service.
- 3 Run the `su postgres` command to become a postgres user.
- 4 Run the command `psql vcac`.
- 5 Set the schema to `saas`.
- 6 Run the following SQL query: `"update "databasechangeloglock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`

- 7 Run the SQL query `select * from databasechangeloglock`.
The output should show a value of "f" for locked.
- 8 Start the horizon-workspace service using the command `service horizon-workspace start`.

Incorrect Appliance Role Assignments After Failover

After a failover occurs, master and replica vRealize Automation appliance nodes might not have the correct role assignment, which affects all services that require database write access.

Problem

In a high availability cluster of vRealize Automation appliances, you shut down or make the master database node inaccessible. You use the management console on another node to promote that node as the new master, which restores vRealize Automation database write access.

Later, you bring the old master node back online, but the Database tab in its management console still lists the node as the master node even though it is not. Attempts to use any node management console to clear the problem by officially promoting the old node back to master fail.

Solution

When failover occurs, follow these guidelines when configuring old versus new master nodes.

- Before promoting another node to master, remove the previous master node from the load balancer pool of vRealize Automation appliance nodes.
- To have vRealize Automation bring an old master node back to the cluster, let the old machine come online. Then, open the new master management console. Look for the old node listed as `invalid` under the Database tab, and click its **Reset** button.

After a successful reset, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.

- To manually bring an old master node back to the cluster, bring the machine online, and join it to the cluster as if it were a new node. While joining, specify the newly promoted node as the primary node.

After successfully joining, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.

- Until you correctly reset or rejoin an old master node to the cluster, do not use its management console for cluster management operations, even if the node came back online.
- After you correctly reset or rejoin, you may promote an old node back to master.

Failures After Promotion of Replica and Master Nodes

A disk space issue, along with the promotion of replica and master vRealize Automation appliance database nodes, might cause provisioning problems.

Problem

The master node runs out of disk space. You log in to its management interface Database page, and promote a replica node with enough space to become the new master. Promotion appears to succeed when you refresh the management interface page, even though an error message occurred.

Later, on the node that was the old master, you free up the disk space. After you promote the node back to master, however, provisioning operations fail by being stuck `IN_PROGRESS`.

Cause

vRealize Automation cannot properly update the old master node configuration when the problem is not enough space.

Solution

If the management interface displays errors during promotion, temporarily exclude the node from the load balancer. Correct the node problem, for example by adding disk, before re-including it on the load balancer. Then, refresh the management interface Database page and verify that the right nodes are master and replica.

Incorrect vRealize Automation Component Service Registrations

The vRealize Automation appliance management interface can help you resolve registration problems with vRealize Automation component services.

Problem

Under normal operation, all vRealize Automation component services must be unique and in a REGISTERED state. Any other set of conditions might cause vRealize Automation to behave unpredictably.

Cause

The following are examples of problems that might occur with vRealize Automation component services.

- A service has become inactive.
- Server settings caused a service to be in a state other than REGISTERED.
- A dependency on another service caused a service to be in a state other than REGISTERED.
- There are duplicate services.

Solution

Unregister and, where needed, re-register component services that appear to have problems.

- 1 Log in to the vRealize Automation appliance management interface as root.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Click **Services**.
- 3 In the list of services, select a service that is a duplicate, is not in the correct state, or has other problems.
- 4 At the upper right, click **Unregister**.
- 5 To have vRealize Automation re-register the service, log in to a console session on the vRealize Automation appliance as root, and restart vRealize Automation by entering the following command.

```
service vcac-server restart
```


If there are services associated with the embedded vRealize Orchestrator instance, enter the following additional command.

```
service vco-restart restart
```
- 6 To re-register any services associated with an external system, such as an external vRealize Orchestrator instance, log in to the external system and restart the services there.

Troubleshooting IaaS Components

The troubleshooting topics for vRealize Automation IaaS components provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Validating Server Certificates for IaaS

You can use the `vcac-Config.exe` command to verify that an IaaS server accepts vRealize Automation appliance and SSO appliance certificates.

Problem

You see authorization errors when using IaaS features.

Cause

Authorization errors can occur when IaaS does not recognize security certificates from other components.

Solution

- 1 Open a command prompt as an administrator and navigate to the Cafe directory at `<vra-installation-dir>\Server\Model Manager Data\Cafe`, typically `C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Type a command of the form `Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v`. Optional parameters are `-su [SQL user name]` and `-sp [password]`.

If the command succeeds you see the following message:

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

If the command fails, you see a detailed error message.

NOTE This command is available only on the node for the Model Manager Data component.

Credentials Error When Running the IaaS Installer

When you install IaaS components, you get an error when entering your virtual appliance credentials.

Problem

After providing credentials in the IaaS installer, an `org.xml.sax.SAXParseException` error appears.

Cause

You used incorrect credentials or an incorrect credential format.

Solution

- ◆ Ensure that you use the correct tenant and user name values.

For example, the SSO default tenant uses domain name such as `vsphere.local`, not `administrator@vsphere.local`.

Save Settings Warning Appears During IaaS Installation

Message appears during IaaS Installation. Warning: Could not save settings to the virtual appliance during IaaS installation.

Problem

An inaccurate error message indicating that user settings have not been saved appears during IaaS installation.

Cause

Communication or network problems can cause this message to appear erroneously.

Solution

Ignore the error message and proceed with the installation. This message should not cause the setup to fail.

Website Server and Distributed Execution Managers Fail to Install

Your installation of the vRealize Automation appliance infrastructure Website server and Distributed Execution Managers cannot proceed when the password for your IaaS service account contains double quotation marks.

Problem

You see a message telling you that installation of the vRealize Automation appliance Distributed Execution Managers (DEMs) and Website server has failed because of invalid msixexec parameters.

Cause

The IaaS service account password uses a double quotation mark character.

Solution

- 1 Verify that your IaaS service account password does not include double quotation marks as part of the password.
- 2 If your password contains double quotation marks, create a new password.
- 3 Restart the installation.

IaaS Authentication Fails During IaaS Web and Model Management Installation

When running the Prerequisite Checker, you see a message that the IIS authentication check has failed.

Problem

The message tells you that authentication is not enabled, but the IIS authentication check box is selected.

Solution

- 1 Clear the Windows authentication check box.
- 2 Click **Save**.
- 3 Select the Windows authentication check box.
- 4 Click **Save**.
- 5 Rerun the Prerequisite Checker.

Failed to Install Model Manager Data and Web Components

Your vRealize Automation installation can fail if the IaaS installer is unable to save the Model Manager Data component and Web component.

Problem

Your installation fails with the following message:

The IaaS installer failed to save the Model Manager Data and Web components.

Cause

The failure has several potential causes.

- Connectivity issues to the vRealize Automation appliance or connectivity issues between the appliances. A connection attempt fails because there was no response or the connection could not be made.
- Trusted certificate issues in IaaS when using a distributed configuration.
- A certificate name mismatch in a distributed configuration.
- The certificate may be invalid or an error on the certificate chain might exist.
- The Repository Service fails to start.
- Incorrect configuration of the load balancer in a distributed environment.

Solution

■ Connectivity

Verify that you can connect to the vRealize Automation URL in a Web browser.

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

■ Trusted Certificate Issues

- In IaaS, open Microsoft Management Console with the command `mmc.exe` and check that the certificate used in the installation has been added to the Trusted Root Certificate Store in the machine.
- From a Web browser, check the status of the MetaModel service and verify that no certificate errors appear:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

■ Certificate Name Mismatch

This error can occur when the certificate is issued to a particular name and a different name or IP address is used. You can suppress the certificate name mismatch error during installation by selecting **Suppress certificate mismatch**.

You can also use the Suppress certificate mismatch option to ignore remote certificate revocation list match errors.

■ Invalid Certificate

Open Microsoft Management Console with the command `mmc.exe`. Check that the certificate is not expired and that the status is correct. Do this for all certificates in the certificate chain. You might have to import other certificates in the chain into the Trusted Root Certificate Store when using a Certificate hierarchy.

- Repository Service

Use the following actions to check the status of the repository service.

- From a Web browser, check the status of the MetaModel service:
<https://FQDN-or-IP/repository/data/MetaModel.svc>
- Check the `Repository.log` for errors.
- Reset IIS (`iisreset`) if you have problems with the applications hosted on the Web site (Repository, vRealize Automation, or WAPI).
- Check the Web site logs in `%SystemDrive%\inetpub\logs\LogFiles` for additional logging information.
- Verify that Prerequisite Checker passed when checking the requirements.
- On Windows 2012, check that WCF Services under .NET Framework is installed and that HTTP activation is installed.

IaaS Windows Servers Do Not Support FIPS

An installation cannot succeed when Federal Information Processing Standard (FIPS) is enabled.

Problem

Installation fails with the following error while installing the IaaS Web component.

This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

Cause

vRealize Automation IaaS is built on Microsoft Windows Communication Foundation (WCF), which does not support FIPS.

Solution

On the IaaS Windows server, disable the FIPS policy.

- 1 Go to **Start > Control Panel > Administrative tools > Local Security Policy**.
- 2 In the Group Policy dialog, under **Local Policies**, select **Security Options**.
- 3 Find and disable the following entry.

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

Adding an XaaS Endpoint Causes an Internal Error

When you attempt to create an XaaS endpoint, an internal error message appears.

Problem

Creation of an endpoint fails with the following internal error message, *An internal error has occurred*. If the problem persists, please contact your system administrator. When contacting your system administrator, use this reference: `c0DD0C01`. Reference codes are randomly generated and not linked to a particular error message.

Solution

- 1 Open the vRealize Automation appliance log file.
`/var/log/vcac/catalina.out`
- 2 Locate the reference code in the error message.

For example, `c0DD0C01`.

- 3 Search for the reference code in the log file to locate the associated entry.
 - 4 Review the entries that appear above and below the associated entry to troubleshoot the problem.
- The associated log entry does not specifically call out the source of the problem.

Uninstalling a Proxy Agent Fails

Removing a proxy agent can fail if Windows Installer Logging is enabled.

Problem

When you try to uninstall a proxy agent from the Windows Control Panel, the uninstall fails and you see the following error:

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

Cause

This can occur if Windows Installer Logging is enabled, but the Windows Installer engine cannot properly write the uninstallation log file. For more information, see [Microsoft Knowledge Base article 2564571](#).

Solution

- 1 Restart your machine or restart explorer.exe from the Task Manager.
- 2 Uninstall the agent.

Machine Requests Fail When Remote Transactions Are Disabled

Machine requests fail when Microsoft Distributed Transaction Coordinator (DTC) remote transactions are disabled on Windows server machines.

Problem

If you provision a machine when remote transactions are disabled on the Model Manager portal or the SQL Server, the request will not complete. Data collection fails and the machine request remains in a state of CloneWorkflow.

Cause

DTC Remote Transactions are disabled in the IaaS SQL Instance used by the vRealize Automation system.

Solution

- 1 Launch Windows Server Manager to enable DTC on all vRealize servers and associated SQL servers.

In Windows 7, navigate **Start > Administrative Tools > Component Services**.

NOTE Ensure that all Windows servers have unique SIDs for MSDTC configuration.

- 2 Open all nodes to locate the local DTC, or the clustered DTC if using a clustered system.
Navigate **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.
- 3 Right click on the local or clustered DTC and select **Properties**.
- 4 Click the Security tab.
- 5 Select the **Network DTC Access** option.
- 6 Select the **Allow Remote Client** and **Allow Remote Administration** options.
- 7 Select the **Allow Inbound** and **Allow Outbound** options.
- 8 Enter or select NT AUTHORITY\Network Service in the **Account** field for the DTC Logon Account.

- 9 Click **OK**.
- 10 Remove machines that are stuck in the Clone Workflow state.
 - a Log in to the vRealize Automation product interface.
`https://vrealize-automation-appliance-FQDN/vcac/tenant-name`
 - b Navigate to **Infrastructure > Managed Machines**.
 - c Right click the target machine.
 - d Select **Delete** to remove the machine.

Error in Manager Service Communication

IaaS nodes that are cloned from a template on which MS DTC is installed contain duplicate identifiers for MS DTC, which prevents communication among the nodes.

Problem

The IaaS Manager Service fails and displays the following error in the manager service log.

```
Communication with the underlying transaction manager has failed. --->
System.Runtime.InteropServices.COMException: The MSDTC transaction manager was
unable to pull the transaction from the source transaction manager due to
communication problems. Possible causes are: a firewall is present and it
doesn't have an exception for the MSDTC process, the two machines cannot
find each other by their NetBIOS names, or the support for network transactions
is not enabled for one of the two transaction managers.
```

Cause

When you clone an IaaS node that has MS DTC installed, then both clones use the same unique identifier for MS DTC. Communication between the nodes fails.

Solution

- 1 Open an Administrator command prompt.
- 2 Run the following command: `msdtc -uninstall`
- 3 Reboot the virtual machine.
- 4 Open a separate command prompt and run the following command:
`msdtc -install <manager-service-host>`.

Email Customization Behavior Has Changed

In vRealize Automation 6.0 or later, only notifications generated by the IaaS component can be customized by using the email template functionality from earlier versions.

Solution

You can use the following XSLT templates:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff

- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

Email templates are located in the `\Templates` directory under the server installation directory, typically `%SystemDrive%\Program Files x86\VMware\VCAC\Server`. The `\Templates` directory also includes XSLT templates that are no longer supported and cannot be modified.

Troubleshooting Log-In Errors

The troubleshooting topics for log-in errors for vRealize Automation provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Attempts to Log In as the IaaS Administrator with Incorrect UPN Format Credentials Fails with No Explanation

You attempt to log in to vRealize Automation as an IaaS administrator and are redirected to the login page with no explanation.

Problem

If you attempt to log in to vRealize Automation as an IaaS administrator with UPN credentials that do not include the `@yourdomain` portion of the user name, you are logged out of SSO immediately and redirected to the login page with no explanation.

Cause

The UPN entered must adhere to a `yourname.admin@yourdomain` format, for example if you log in using `jsmith.admin@sqa.local` as the user name but the UPN in the Active Directory is only set as `jsmith.admin`, the login fails.

Solution

To correct the problem change the `userPrincipalName` value to include the needed `@yourdomain` content and retry login. In this example the UPN name should be `jsmith.admin@sqa.local`. This information is provided in the log file in the `log/vcac` folder.

Log In Fails with High Availability

When you have more than one vRealize Automation appliance, the appliances must be able to identify each other by short hostname. Otherwise, you cannot log in.

Problem

You configure vRealize Automation for high availability by installing an additional vRealize Automation appliance. When you try to log in to vRealize Automation, a message about an invalid license appears. The message is incorrect though, because you determined that your license is valid.

Cause

The vRealize Automation appliance nodes do not correctly form a high availability cluster until they can resolve the short hostnames of the nodes in the cluster.

Solution

To allow a cluster of high availability vRealize Automation appliances to resolve short hostnames, take any of the following approaches. You must modify all appliances in the cluster.

Procedure

- Edit or create a search line in `/etc/resolv.conf`. The line should contain domains that hold vRealize Automation appliances. Separate multiple domains with spaces. For example:


```
search sales.mycompany.com support.mycompany.com
```
- Edit or create domain lines in `/etc/resolv.conf`. Each line should contain a domain that holds vRealize Automation appliances. For example:


```
domain support.mycompany.com
```
- Add lines to the `/etc/hosts` file so that each vRealize Automation appliance short name is mapped to its fully qualified domain name. For example:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

Proxy Prevents VMware Identity Manager User Log In

Configuring to use a proxy might prevent VMware Identity Manager users from logging in.

Problem

You configure vRealize Automation to access the network through a proxy server, and VMware Identity Manager users see the following error when they attempt to log in.

```
Error Unable to get metadata
```

Solution**Prerequisites**

Configure vRealize Automation to access the network through a proxy server. See [“Connect to the Network Through a Proxy Server,”](#) on page 132.

Procedure

- 1 Log in to the console of the vRealize Automation appliance as root.
- 2 Open the following file in a text editor.


```
/etc/sysconfig/proxy
```
- 3 Update the `NO_PROXY` line to ignore the proxy server for VMware Identity Manager logins.


```
NO_PROXY=vrealize-automation-hostname
```

 For example: `NO_PROXY=localhost, 127.0.0.1, automation.mycompany.com"`
- 4 Save and close proxy.
- 5 Restart the Horizon workspace service by entering the following command.


```
service horizon-workspace restart
```


Silent vRealize Automation Installation

7

vRealize Automation includes an option for scripted, silent installation.

Silent installation uses an executable that references a text-based answer file, in which you preconfigure system FQDNs, account credentials, and other settings that you typically add throughout a conventional wizard-based or manual installation. Silent installation is useful for the following kinds of deployments.

- Deploying multiple, nearly identical environments
- Repeatedly redeploying the same environment
- Performing unattended installations
- Performing scripted installations

This chapter includes the following topics:

- [“Perform a Silent vRealize Automation Installation,”](#) on page 147
- [“Perform a Silent vRealize Automation Management Agent Installation,”](#) on page 148
- [“Silent vRealize Automation Installation Answer File,”](#) on page 149
- [“The vRealize Automation Installation Command Line,”](#) on page 149
- [“The vRealize Automation Installation API,”](#) on page 151
- [“Convert Between vRealize Automation Silent Properties and JSON,”](#) on page 152

Perform a Silent vRealize Automation Installation

You can perform an unattended, silent vRealize Automation installation from the console of a newly deployed vRealize Automation appliance.

Prerequisites

- Deploy a vRealize Automation appliance, but do not log in and start the Installation Wizard.
- Create or identify your IaaS Windows servers, and configure their prerequisites.
- Install the Management Agent on your IaaS Windows servers.

You may install the Management Agent using the traditional .msi file download or the silent process described in [“Perform a Silent vRealize Automation Management Agent Installation,”](#) on page 148.

Procedure

- 1 Log in to the vRealize Automation appliance console as root.

- 2 Navigate to the following directory.

```
/usr/lib/vcac/tools/install
```

- 3 Open the `ha.properties` answer file in a text editor.
- 4 Add entries specific to your deployment in `ha.properties`, and save and close the file.

Alternatively, you can save time by copying and modifying an `ha.properties` file from another deployment instead of editing the entire default file.

- 5 From the same directory, start the installation by running the following command.

```
vra-ha-config.sh
```

Installation might take up to an hour or more to complete, depending on the environment and size of the deployment.

- 6 (Optional) After installation finishes, review the log file.

```
/var/log/vcac/vra-ha-config.log
```

The silent installer does not save proprietary data to the log, such as passwords, licenses, or certificates.

Perform a Silent vRealize Automation Management Agent Installation

You can perform a command line based vRealize Automation Management Agent installation on any IaaS Windows server.

Silent Management Agent installation consists of a Windows PowerShell script in which you customize a few settings. After adding your deployment-specific settings, you can silently install the Management Agent on all of your IaaS Windows servers by running copies of the same script on each one.

Prerequisites

- Deploy the vRealize Automation appliance.
- Create or identify your IaaS Windows servers, and configure their prerequisites.

Procedure

- 1 Log in to the IaaS Windows server using an account that has administrator rights.
- 2 Open a Web browser to the vRealize Automation appliance installer URL.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Right-click the link to the `InstallManagementAgent.ps1` PowerShell script file, and save it to the desktop or a folder on the IaaS Windows server.
- 4 Open `InstallManagementAgent.ps1` in a text editor.
- 5 Near the top of the script file, add your deployment-specific settings.
 - The vRealize Automation appliance URL
`https://vrealize-automation-appliance-FQDN:5480`
 - vRealize Automation appliance root user account credentials
 - vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers
 - The folder where you want to install the Management Agent, `Program Files (x86)` by default
 - (Optional) The thumbprint of the PEM format certificate that you are using for authentication
- 6 Save and close `InstallManagementAgent.ps1`.

- 7 To silently install the Management Agent, double-click `InstallManagementAgent.ps1`.
- 8 (Optional) Verify that installation has finished by locating **VMware vCloud Automation Center Management Agent** in the Windows Control Panel list of Programs and Features, and in the list of Windows services that are running.

Silent vRealize Automation Installation Answer File

Silent vRealize Automation installations require that you prepare a text-based answer file in advance.

All newly deployed vRealize Automation appliances contain a default answer file.

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

To perform a silent installation, you must use a text editor to customize the settings in `ha.properties` to the deployment that you want to install. The following examples are a few of the settings and information that you must add.

- Your vRealize Automation or suite license key
- vRealize Automation appliance node FQDNs
- vRealize Automation appliance root user account credentials
- IaaS Windows server FQDNs that will act as Web nodes, Manager Service nodes, and so on
- vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers
- Load balancer FQDNs
- SQL Server database parameters
- Proxy agent parameters to connect to virtualization resources
- Whether the silent installer should attempt to correct missing IaaS Windows server prerequisites

The silent installer can correct many missing Windows prerequisites. However, some configuration problems, such as not enough CPU, cannot be changed by the silent installer.

To save time, you can reuse and modify an `ha.properties` file that was configured for another deployment, one where the settings were similar. Also, when you install vRealize Automation non-silently through the Installation Wizard, the wizard creates and saves your settings in the `ha.properties` file. The file might be useful to reuse and modify for silently installing a similar deployment.

The wizard does not save proprietary settings to the `ha.properties` file, such as passwords, licenses, or certificates.

The vRealize Automation Installation Command Line

vRealize Automation includes a console-based, command line interface for performing installation adjustments that might be required after initial installation.

The command line interface (CLI) can run installation and configuration tasks that are no longer available through the browser-based interface after initial installation. CLI features include rechecking prerequisites, installing IaaS components, installing certificates, or setting the vRealize Automation host name to which users point their Web browser.

The CLI is also useful for advanced users who want to script certain operations. Some CLI functions are used by silent installation, so familiarity with both features reinforces your knowledge of vRealize Automation installation scripting.

vRealize Automation Installation Command Line Basics

The vRealize Automation installation command line interface includes top-level, basic operations.

The basic operations display vRealize Automation node IDs, run commands, report command status, or display the help information. To show these operations and all of their options at the console display, enter the following command without any options or qualifiers.

```
vra-command
```

Display Node IDs

You need to know vRealize Automation node IDs in order to run commands against the correct target systems. To display node IDs, enter the following command.

```
vra-command list-nodes
```

Make note of node IDs before running commands against specific machines.

Run Commands

Most command line functions involve running a command against a node in the vRealize Automation cluster. To run a command, use the following syntax.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

As shown in the preceding syntax, many commands require parameters and parameter values chosen by the user.

Display Command Status

Some commands take a few moments or even longer to complete. To check the progress of a command that was entered, enter the following command.

```
vra-command status
```

The status command is especially valuable for monitoring a silent install, which can take a long time for large deployment sizes.

Display Help

To display help information for all available commands, enter the following command.

```
vra-command help
```

To display help for a single command, enter the following command.

```
vra-command help command-name
```

vRealize Automation Installation Command Names

Commands give you console access to many vRealize Automation installation and configuration tasks that you might want to perform after initial installation.

Examples of available commands include the following functions.

- Adding another vRealize Automation appliance to an existing installation
- Setting the host name that users point a Web browser to when they access vRealize Automation
- Creating the IaaS SQL Server database
- Running the prerequisite checker against an IaaS Windows server
- Importing certificates

For a complete list of available vRealize Automation commands, log in to the vRealize Automation appliance console, and enter the following command.

```
vra-command help
```

The long list of command names and parameters is not reproduced in separate documentation. To use the list effectively, identify a command of interest, and narrow your focus by entering the following command.

```
vra-command help command-name
```

The vRealize Automation Installation API

The vRealize Automation REST API for installation gives you the ability to create purely software-controlled installations for vRealize Automation.

The installation API requires a JSON formatted version of the same entries that the CLI based installation obtains from the `ha.properties` answer file. The following guidelines familiarize you with how the API works. From there, you should be able to design programmatic calls to the API to install vRealize Automation.

- To access the API documentation, point a Web browser to the following vRealize Automation appliance page.

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

- To experiment with the API based installation, locate and expand the following PUT command.

```
PUT /vra-install
```

- Copy the unpopulated JSON from the **install_json** box to a text editor. Fill in the answer values the same way that you would for `ha.properties`. When your JSON formatted answers are ready, copy the code back to **install_json** and overwrite the unpopulated JSON.

Alternatively, you can edit the following template JSON and copy the result to **install_json**.

```
/usr/lib/vcac/tools/install/installationProperties.json
```

You can also convert a completed `ha.properties` to JSON or vice versa.

- In the action box, select **validate** and click **Try It Out**.

The validate action runs the vRealize Automation prerequisite checker and fixer.

- The validate response includes an alphanumeric command ID that you can insert into the following GET command.

```
GET /commands/command-id/aggregated-status
```

The response to the GET includes the progress of the validation operation.

- When validation succeeds, you can run the actual installation by repeating the process. In the action box, just select **install** instead of **validate**.

Installation can take a long time depending on the deployment size. Again, locate the command ID, and use the aggregated status GET command to obtain installation progress. The GET response might resemble the following example.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18, "queued": 3,
"processing": 1}, "failed-commands": 0
```

- If something goes wrong with the installation, you can trigger log collection for all nodes using the following command.

```
PUT /commands/log-bundle
```

Similar to installation, the returned alphanumeric command ID lets you monitor log collection status.

Convert Between vRealize Automation Silent Properties and JSON

For silent vRealize Automation CLI or API based installations, you can convert a completed properties answer file to JSON or vice versa. The silent CLI installation requires the properties file, while the API requires JSON format.

Prerequisites

A completed properties answer file or completed JSON file

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

or

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Procedure

- 1 Log in to a vRealize Automation appliance console session as root.
- 2 Run the appropriate converter script.

- Convert JSON to Properties

```
/usr/lib/vcac/tools/install/convert-properties --from-json installationProperties.json
```

The script creates a new properties file with the timestamp in the name, for example:

```
ha.2016-10-17_13.02.15.properties
```

- Convert Properties to JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

The script creates a new installationProperties.json file with the timestamp in the name, for example:

```
installationProperties.2016-10-17_13.36.13.json
```

You can also display help for the script.

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

Index

A

- account settings, specifying **58**
- agents
 - choosing the installation scenario **98**
 - configuring Hyper-V **107**
 - configuring vSphere agents **103**
 - configuring XenServer **107**
 - enabling remote WMI requests **117**
 - Hyper-V **104**
 - installation location and requirements **99**
 - installing **97**
 - installing WMI **117**
 - installing XenDesktop **109**
 - installing Citrix agents **112**
 - installing EPI agent for Citrix **111**
 - installing for Visual Basic scripting **115**
 - installing the EPI agent for VB scripting **114**
 - installing vSphere agents **101**
 - Visual Basic scripting requirements **114**
 - XenServer **104**
- answer file, silent installation **149**
- API, installation **151**
- API (application programming interface) **151**
- appliance, host name change **122, 123**
- appliances, configuring additional **72**
- application programming interface (API) **151**
- authentication **96**

C

- CEIP (Customer Experience Improvement Program) **39**
- certificate chains, order **30**
- certificate validation **138**
- certificate name mismatch **140**
- certificates
 - switching from self-signed **122**
 - trust relationships **63**
- chained certificates, order **30**
- Citrix, installing the EPI agent **111**
- Citrix agents, installing **112**
- Cloned IaaS nodes **143**
- clusters;joining **72**
- command line **149, 150**
- component service registrations **137**
- configure, vRealize Automation appliance **69**

- Customer Experience Improvement Program (CEIP) **39**

D

- database
 - creating by using the wizard **79**
 - preparing IaaS database **77**
 - requirements **21**
- DEM
 - about installing **92**
 - installing **93**
 - Ooemstack requirements **25**
 - PowerVC requirements **25**
 - requirements **23**
- DEM Worker **25, 94**
- DEM (Distributed Execution Manager) **12**
- dems
 - Amazon Web Services EC2 requirements **24**
 - Red Hat requirements **25**
- DEMs, install fails **139**
- deployment
 - distributed **16**
 - minimal **15, 35**
- deployment parameters, specifying **39, 46**
- deployment scenario
 - distributed deployment **60**
 - minimal deployment **49**
 - minimal installation **14**
- deployment path
 - choosing **14**
 - distributed installation **14**
- disk space **136**
- distributed deployment
 - disable unused services **73**
 - install with wizard **41**
 - validating **74**
- Distributed Execution Managers, *See also* DEM
- distributed installation
 - overview **60**
 - uninstalling **129**
- Distributed Transaction Coordinator (DTC) **21**
- Distributed Execution Manager, *See* DEM
- Distributed Execution Manager (DEM) **12**
- DTC (Distributed Transaction Coordinator) **21**

E

- Email customizations **143**
- Encryption.key file, setting permissions **134**
- Endpoints
 - Ooemstack DEM requirements **25**
 - PowerVC DEM requirements **25**
- Enterprise deployment, install with wizard **41**
- EPI agents, installing for Visual Basic scripting **114, 115**
- external provisioning integration agents **13**

F

- failed installation, logs **127**
- Federal Information Processing Standard (FIPS) **121, 141**
- FIPS (Federal Information Processing Standard) **121, 141**

H

- ha.properties **152**
- health checks **62**
- host name change
 - master appliance **122**
 - replica appliance **123**
- Hyper-V
 - agent **104**
 - proxy agent **104**
 - requirements **104**
- Hyper-V agents, installing **104**
- hypervisor, requirements **104**

I

- laaS
 - agents **13**
 - Distributed Execution Manager **12**
 - download installer **76**
 - Manager Service **12**
 - Model Manager **12**
 - SQL Server database **12**
 - Web server **12**
- laaS (Infrastructure as a Service) **12**
- laaS administrators, creating **124**
- laaS components
 - installing **55**
 - installing in a distributed configuration **74**
 - registering **59**
 - troubleshooting **138**
- laaS components, definitions **61**
- laaS installer
 - downloading **57**
 - troubleshooting **138**
- laaS services, verifying **97**
- laaS Authentication, failure **139**
- laaS administrator login fails **144**

- laaS database
 - configuring for secure SSL **58, 77–79**
 - configuring Windows service for access **95**
 - creating the database **78**
 - creating the database manually **77**
 - creating the database using the wizard **79**
 - specifying the SQL database **58**
- laaS database access, enabling from service user **96**
- laaS distributed installation **61**
- laaS Manager Service, requirements **23**
- identity manager, fails to start **135**
- identity store, domain requirements **28**
- infrastructure components, installing **56**
- Infrastructure as a Service (laaS) **12**
- Initial content configuration, create password **40, 48**
- initial content creation, troubleshooting **133**
- installation
 - API **151**
 - completing **60**
 - distributed **16**
 - DNS and host name resolution **19**
 - finishing **46**
 - minimal **15, 35**
 - minimal installation overview **49**
 - overview **11**
 - post-installation **121**
 - preparation **19**
 - specifying agents **59**
 - specifying managers **59**
 - troubleshooting **127**
 - vRealize Automation appliance **50, 68**
- Installation, using the management console **49**
- installation components
 - checking prerequisites **58**
 - choosing a deployment path **14**
- installation method **17**
- installation parameter, validation **40, 47**
- installation preparation, time synchronization **31**
- installation requirements
 - credentials **28**
 - deployment environments **20**
 - hardware **20**
 - laaS requirements **22**
 - operating system **20**
 - port requirements **26**
 - security **30**
 - users **28**
 - virtual machine **20**
 - Windows server **21**
 - XenDesktop **108**
- Installation troubleshooting **130**

installation wizard, enterprise deployment **41**
 Installation Wizard, overview **33**
 installation download, troubleshooting **134**
 installation failure, servers out of sync **131**
 installation type
 logging in **57**
 selecting **57**
 installing
 browser considerations **20**
 configuring vCloud Automation Center
 Appliances **68**
 download IaaS installer **76**
 worksheet **64**
 internal error, adding XaaS endpoint **141**

J

Java requirements, for MSSQL database **22**
 JSON **152**

K

key **39**
 keys **134**

L

license key **39**
 licenses **134**
 load balancer times out before completion,
 changing the load balancer timeout
 setting **130**
 load balancers
 configuring **68**
 health checks **62**
 Log Insight **124**
 Log in errors, troubleshooting **144**
 login failure
 servers out of sync **131**
 troubleshooting **144**
 logs
 collecting **130**
 locations **127**
 Logs
 IaaS **127**
 troubleshooting **127**

M

machine request fails **142**
 Management Agent
 installing **35, 42**
 silent installation **148**
 Management Agent SSL fingerprint, locating **36,**
 42
 Manager service, definition **61**
 Manager Service
 installing **87, 90**
 requirements **23**

manager service, certificate trust **63**
 master appliance, host name change **122**
 master node incorrect **136**
 master nodes **136**
 minimal deployment **35**
 minimal installation, uninstalling **128**
 Model Manager
 definition **61**
 troubleshooting install failures **140**
 Model Manager data, installing **81, 83, 85**

N

node IDs **150**

O

Openstack, DEM requirements **25**

P

password, restrictions **21**
 PEM files, command for extracting **30**
 pfx files, configure certificate trust **63**
 post-installation **121**
 post-installation tasks, configuring Windows
 service to access IaaS database **95**
 PowerShell, setting to RemoteSigned **98**
 PowerVC, DEM requirements **25**
 Prerequisite Checker, run in Installation
 Wizard **38, 45**
 prerequisites
 browser considerations **20**
 checking **58**
 product license key **39**
 provisioning server **111**
 proxy **145**
 proxy agent, uninstall fails **142**
 proxy agents, installing and configuring for
 vSphere **99**

R

registration, services **137**
 replica appliance, host name change **123**
 replica nodes **136**
 requirements
 database **21**
 DEM **23**
 SQL **21**
 REST API **151**
 RSA private keys, command for extracting **30**
 run-time authentication **96**

S

scenarios, choosing the agent installation **98**
 SCVMM **25, 94**
 security
 certificates **30**

- laaS certificates **56, 75**
 - passphrase **31**
 - third-party software **31**
 - trust relationships **63**
- server settings, specifying **58**
- server requirements, laaS or Windows server **22**
- service registrations **137**
- silent installation
 - answer file **149**
 - JSON converter **152**
 - Management Agent **148**
 - properties converter **152**
 - use cases **147**
 - vRealize Automation **147**
- snapshots, creating **39, 46**
- SQL, requirements **21**
- SQL authentication **96**
- SQL Server database **12**
- SSL **132**
- SSL certificates, extracting **30**
- support bundle, creating **130**
- System error message **134**

T

- telemetry **39**
- tenants, configuring default tenant **124**
- time synchronize, servers **52, 72**
- time sync, enabling on Windows machine **55**
- TLS **132**
- troubleshooting
 - blank pages appearing **131**
 - cloned laaS nodes **143**
 - laaS installer **138**
 - log locations **127**
 - machine requests **142**
 - master node incorrect **136**
 - server times out of sync **131**
- troubleshooting, installation **127**
- trusted certificate issues **140**

U

- uninstall, failed installation **128, 129**
- Uninstall, failed installation **128**
- updated information **9**
- use cases, silent installation **147**

V

- vCloud Suite, licensing **7**
- VDI agent for XenDesktop, installing **108**
- virtual appliance time settings, with the Installation Wizard **38, 44**
- virtual desktop integration agents **13**
- virtualization proxy agents **13**
- Visual Basic, scripting requirements **114**

- Visual Basic scripting
 - installing EPI agents **115**
 - installing the EPI agent **114**
- VMware Identity Manager **145**
- vRealize Appliance
 - configuring **52**
 - deploying **33, 50**
- vRealize Automation appliance, deploying **66**
- vRealize Orchestrator, use external for high-availability deployments **60**
- vRealize Realize Automation appliance **50**
- vRealize Appliance clusters;joining **72**
- vRealize Automation appliances, troubleshooting **134**
- vSphere agents
 - configuring **103**
 - installing **101**
 - requiring a trusted certificate **103**
- vSphere agent
 - required permissions **99**
 - supported configuration for concurrency **99**
- vSphere proxy agents, installing and configuring **99**

W

- WAPI, install fails **139**
- Web server **12**
- website component, installing **81, 83, 85**
- Windows authentication **96**
- Windows Management Instrumentation (WMI) **13**
- WMI (Windows Management Instrumentation) **13**
- WMI agents
 - enabling remote requests **117**
 - installing **117**

X

- XenDesktop
 - installation requirements **108**
 - installing agent **109**
 - installing VDI agent **108**
- XenServer
 - agent **104**
 - proxy agent **104**
- XenServer agents, installing **104**
- XenServer Host name, setting **109**