Installing vRealize Automation

vRealize Automation 7.0.1

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.
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
Contents

vRealize Automation Installation 7

Updated Information 9

1 vRealize Automation Installation Overview 11
   Choosing Your Deployment Path 11
   Minimal Deployment Overview 12
   Enterprise Deployment Overview 13
   vRealize Automation Installation Components 14
   VMware vRealize Automation Appliance 15
   Management Agents 15
   vRealize Automation Infrastructure as a Service 15

2 Preparing for Installation 19
   DNS and Host Name Resolution 19
   Hardware and Virtual Machine Requirements 19
   Browser Considerations 20
   Password Considerations 20
   Windows Server Requirements 21
      IaaS Database Server Requirements 21
      IaaS Web Service and Model Manager Server Requirements 21
      IaaS Manager Service 22
      Distributed Execution Manager Requirements 23
   Port Requirements 24
   User Accounts and Credentials Required for Installation 26
   Security 28
      Certificates 28
      Extracting Certificates and Private Keys 28
      Security Passphrase 29
      Third-Party Software 29
      Time Synchronization 29

3 Installing vRealize Automation with the Installation Wizard 31
   Deploy the vRealize Automation Appliance 31
   Installing a Minimal Deployment with the Installation Wizard 32
      Run the Installation Wizard for a Minimal Deployment 33
      Installing the Management Agent 34
      Synchronize Server Times 36
      Run the Prerequisite Checker 36
   Specify Deployment Configuration Parameters 37
   Create Snapshots Before You Begin the Installation 37
   Scenario: Finish the Installation 38
Address Installation Failures 38
Set Up Credentials for Initial Content Configuration 39
Installing an Enterprise Deployment with the Installation Wizard 40
Run the Installation Wizard for an Enterprise Deployment 40
Installing the Management Agent 40
Synchronize Server Times 43
Run the Prerequisite Checker 43
Specify Deployment Configuration Parameters 44
Create Snapshots Before You Begin the Installation 44
Finish the Installation 45
Address Installation Failures 45
Set Up Credentials for Initial Content Configuration 46

4 Installing vRealize Automation through the Standard Interfaces 47
Minimal Deployment 47
  Minimal Deployment Checklist 47
  Deploy and Configure the vRealize Automation Appliance 48
  Installing IaaS Components 52
Distributed Deployment 57
  Distributed Deployment Checklist 57
  Distributed Installation Components 58
  Certificate Trust Requirements in a Distributed Deployment 59
  Installation Worksheets 60
  Deploy the vRealize Automation Appliance 61
  Configuring Your Load Balancer 63
  Configuring Appliances for vRealize Automation 63
  Install the IaaS Components in a Distributed Configuration 69
Installing Agents 91
  Set the PowerShell Execution Policy to RemoteSigned 91
  Choosing the Agent Installation Scenario 92
  Agent Installation Location and Requirements 92
  Installing and Configuring the Proxy Agent for vSphere 92
  Installing the Proxy Agent for Hyper-V or XenServer 97
  Installing the VDI Agent for XenDesktop 101
  Installing the EPI Agent for Citrix 104
  Installing the EPI Agent for Visual Basic Scripting 106
  Installing the WMI Agent for Remote WMI Requests 109

5 Configure Access to the Default Tenant 113

6 Replacing Self-Signed Certificates with Certificates Provided by an Authority 115

7 Troubleshooting 117
  Default Log Locations 117
  Rolling Back a Failed Installation 118
    Roll Back a Minimal Installation 118
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/](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](http://www.vmware.com/support/pubs).
Updated Information

*Installing vRealize Automation 7.0* is updated with each release of the product or when necessary. This table provides the update history of the *Installing vRealize Automation 7.0* publication.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN-001835-03</td>
<td>Additional troubleshooting procedures.</td>
</tr>
<tr>
<td>EN-001835-02</td>
<td>Removed outdated procedures about database failovers, from Chapter 4.</td>
</tr>
</tbody>
</table>
| EN-001835-01 | • Addition of new deployment scenario for installing and configuring a vRealize Automation proof of concept and development environment. For an overview of the example scenario, see “Choosing Your Deployment Path,” on page 11. For the full scenario, see *Installing and Configuring vRealize Automation for the Rainpole Scenario*.  
• Several small updates to clarify that high availability is not fully configured until your tenant administrators set up Directories Management for high availability.  
• Updates for version 7.0.1 of vRealize Automation. |
| EN-001835-00 | Initial document release. |
vRealize Automation can be deployed in a variety of configurations. To ensure a successful deployment understand the deployment and configuration options, and the sequence of tasks required.

If you are familiar with earlier versions of vRealize Automation, it might be helpful to note the following changes before you begin your installation:

- This release of vRealize Automation introduces the Installation Wizard, the recommended method for unscripted installations. With the wizard, you can choose a minimal or enterprise deployment. Enterprise deployments are based on distributed architectures and can include load balancers for high-availability deployments. You can install vRealize Automation appliances alone or with IaaS components.

- Single Sign-On support and identity management is done by means of an embedded VMware Identity Manager that is administered by the new Directories Management feature. This replaces the use of the VMware Identity Appliance and vSphere SSO implementations used by previous product versions.

- Open LDAP is no longer supported.

After installation, system administrators can customize the installation environment and configure one or more tenants, which sets up access to self-service provisioning and life-cycle management of cloud services.

By using the secure portal Web interface, administrators, developers, or business users can request IT services and manage specific cloud and IT resources based on their roles and privileges. Users can request infrastructure, applications, desktops, and IT service through a common service catalog.

This chapter includes the following topics:

- “Choosing Your Deployment Path,” on page 11
- “vRealize Automation Installation Components,” on page 14

Choosing Your Deployment Path

Depending on your deployment requirements, you can install and configure vRealize Automation components by using the rainpole installation scenario, the Installation Wizard, or through the management console.

Choose a minimal installation to deploy a proof of concept (PoC) or development environment with a basic topology. Choose an enterprise installation to deploy a production environment with the topology best suited to your organizational needs.
### Table 1-1. Choosing Your Installation Method

<table>
<thead>
<tr>
<th>Installation Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Wizard</td>
<td>The Installation Wizard provides the quickest installation path for most deployments. You can choose a minimal or enterprise deployment to support distributed components with or without load balancers. Complete and verify all prerequisites before you start the wizard. For more information, see Chapter 2, “Preparing for Installation,” on page 19.</td>
</tr>
<tr>
<td>Manual installation</td>
<td>Installation through the management console is also supported for minimal, distributed, and high-availability installations. Complete and verify all prerequisites before you begin the installation. For more information, see Chapter 2, “Preparing for Installation,” on page 19. <strong>Note</strong> If you use the management console to start or configure any part of your installation, you cannot start or continue use of the Installation Wizard.</td>
</tr>
</tbody>
</table>

### Table 1-2. Choosing Your Deployment Type

<table>
<thead>
<tr>
<th>Deployment Purpose</th>
<th>Choose this deployment type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy a proof of concept (PoC) or development environment with a basic topology.</td>
<td>Install a minimal deployment. You deploy a single instance of vRealize Automation appliance and install all IaaS components on a single Windows server machine. You can install the databases on the same Windows machine or on a dedicated SQL Server.</td>
</tr>
<tr>
<td>Deploy a production environment with the topology best suited to your organizational needs.</td>
<td>Install an enterprise deployment. You distribute components across multiple servers. Optionally, you can deploy load balancers to distribute work across servers and provide fail over capability and redundancy in a high-availability environment.</td>
</tr>
</tbody>
</table>


### Minimal Deployment Overview

To complete a minimal deployment, a system administrator installs the vRealize Automation appliance and Infrastructure as a Service (IaaS) components.

- vRealize Automation appliance includes the Web console interface and support for single sign-on capabilities. It is installed as a virtual appliance.
- Infrastructure as a Service (IaaS) is installed on a Windows Server machine.
- The IaaS uses an SQL database that can be installed on the same machine as IaaS or on its own server.

The following figure shows the relationship and purpose of components of a minimal installation.
Enterprise Deployment Overview

The system administrator can deploy and install multiple instances of the vRealize Automation appliance and individual IaaS components for scale, redundancy, high availability, and disaster recovery.

In a typical architecture, the IaaS components are distributed over multiple machines.

For high availability deployments, load balancers distribute the workload across the computing environment. System administrators configure load balancers outside of the vRealize Automation framework.

The following figure shows the components of an enterprise deployment with distributed components, redundancy, and load balancers.
A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

An installation consists of the following components.

- vRealize Automation appliance, which deploys the management console, manages Single Sign-On (SSO) capabilities for authorization and authentication, and includes an instance of vRealize Orchestrator.
- Infrastructure as a Service (IaaS) components, which are installed on a Windows machine (virtual or physical), and appear largely under the Infrastructure tab on the console.
- An MS SQL Server Database, which is deployed during the IaaS installation.
VMware vRealize Automation Appliance
The vRealize Automation appliance is a preconfigured virtual appliance that contains the vRealize Automation server. vRealize Automation is delivered as an open virtualization format (OVF) template. The system administrator deploys the virtual appliance to an existing virtualized infrastructure.

The server includes the vRealize Automation appliance product console, which provides a single portal for self-service provisioning and management of cloud services, authoring, administration, and governance.

Appliance Database
During deployment of the virtual appliances, a PostgreSQL appliance database is created automatically on the first vRealize Automation appliance. A replica database can be installed on a second vRealize Automation appliance to create a high-availability environment.

Management Agents
Management Agents are stand-alone IaaS components that register IaaS nodes with vRealize Automation appliances, automate the installation and management of IaaS components, and collect support and telemetry information.

A Management Agent must be installed on each Windows machine hosting IaaS components.

vRealize Automation Infrastructure as a Service
Infrastructure as a Service (IaaS) enables the rapid modeling and provisioning of servers and desktops across private, public or hybrid cloud infrastructures.

The system administrator installs IaaS components on a Windows machine. IaaS capabilities are also available from the Infrastructure tab on the management console. IaaS has several components that you can install in a custom configuration to meet the needs of your organization.

IaaS Website
The IaaS Website component provides the infrastructure administration and service authoring capabilities to the vRealize Automation console. The Website component communicates with the Manager Service, which provides it with updates from the Distributed Execution Manager (DEM), proxy agents, and database.

Model Manager
vRealize Automation models facilitate integration with external systems and databases. They implement business logic that a Distributed Execution Manager (DEM) uses.

The Model Manager provides services and utilities for persisting, versioning, securing, and distributing model elements. It communicates with the database, the DEMs, and the console Web site.

vCloud Automation Center Manager Service
The Manager Service coordinates communication between DEMs, agents, and the database. The Manager Service communicates with the console Web site through the Model Manager. This service requires administrative privileges to run.

IaaS Database
The IaaS component of vRealize Automation uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies. Typically, the database is created for you during installation. However, a system administrator can create the database separately as well.
**Distributed Execution Managers**

A Distributed Execution Manager (DEM) runs the business logic of custom models, interacting with the database and with external databases and systems as required.

Each DEM instance acts in either a Worker role or in an Orchestrator role. The Worker role is responsible for running workflows. The Orchestrator role is responsible for monitoring DEM Worker instances, preprocessing workflows to run, and scheduling workflows.

The DEM Orchestrator performs these specific tasks.

- Monitors the status of DEM Workers and ensures that if a Worker instance stops or loses its connection to the Model Manager, its workflows are put back in the queue for another DEM Worker to pick up.
- Manages scheduled workflows by creating new workflow instances at the scheduled time.
- Ensures that only one instance of a particular scheduled workflow is running at a given time.
- Preprocesses workflows before they are run, including checking preconditions for workflows, used in the implementation of the RunOneOnly feature, and creating the workflow execution history.

One DEM Orchestrator instance is designated as the active Orchestrator that performs these tasks. Because the DEM Orchestrator is essential to run workflows, install at least one additional Orchestrator instance on a separate machine for redundancy. The Orchestrator is automatically installed on the machine that also runs the Manager Service. The additional DEM Orchestrator monitors the status of the active Orchestrator so that it can take over if the active Orchestrator goes offline.

**vRealize Automation Agents**

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

You generally install the vSphere agent as part of a deployment. You can install additional agents according to your site’s requirements.

**Integration Agents**

Virtual desktop integration (VDI) PowerShell agents allow vRealize Automation to integrate with external virtual desktop systems. Currently, virtual machines that vRealize Automation provisions can be registered with XenDesktop on a Citrix Desktop Delivery Controller (DDC) and their owners can access the XenDesktop Web Interface from vRealize Automation.

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.

VDI and EPI agents require administrator-level access to the external systems with which they interact.

**Virtualization Proxy Agents**

The virtual machines that vRealize Automation manages are created on virtualization hosts. vRealize Automation uses virtualization proxy agents to send commands to and collect data from vSphere ESX Server, XenServer, and Hyper-V virtualization hosts and the virtual machines provisioned on them. A proxy agent has the following characteristics.

- Typically requires administrator-level access to the virtualization platform it manages
- Communicates with the Manager Service
- Is installed separately with its own configuration file
Windows Management Instrumentation Agent

The vRealize Automation Windows Management Instrumentation (WMI) agent enhances your ability to monitor and control system information and allows you to manage remote servers from a central location. It enables the collection of data from Windows machines that vRealize Automation manages.
Installing vRealize Automation
Preparing for Installation

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:

- “DNS and Host Name Resolution,” on page 19
- “Hardware and Virtual Machine Requirements,” on page 19
- “Browser Considerations,” on page 20
- “Password Considerations,” on page 20
- “Windows Server Requirements,” on page 21
- “Port Requirements,” on page 24
- “User Accounts and Credentials Required for Installation,” on page 26
- “Security,” on page 28
- “Time Synchronization,” on page 29

DNS and Host Name Resolution

vRealize Automation requires the system administrator to identify all hosts by using a fully qualified domain name (FQDN).

In a distributed deployment, all vRealize Automation components must be able to resolve each other by using an FQDN.

The Model Manager Web service, Manager Service, and Microsoft SQL Server database must also be able to resolve each other by their Windows Internet Name Service (WINS) name. You must configure the Domain Name System (DNS) to resolve these host names in your environment.

**Important** vRealize Automation does not allow navigation to hosts that contain the underscore (_) character in the host name.

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

<table>
<thead>
<tr>
<th>vRealize Automation appliance for Small Active Directories</th>
<th>vRealize Automation appliance for Large Active Directories</th>
<th>IaaS Components (Windows Server).</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ 4 CPUs</td>
<td>■ 4 CPUs</td>
<td>■ 2 CPUs</td>
</tr>
<tr>
<td>■ 18 GB memory</td>
<td>■ 22 GB memory</td>
<td>■ 8 GB memory</td>
</tr>
<tr>
<td>■ 60 GB disk storage</td>
<td>■ 60 GB disk storage</td>
<td>■ 30 GB disk storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional resources are required when you are include an SQL Server on a Windows host.</td>
</tr>
</tbody>
</table>

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 vRealize Automation administrator password that you define during installation must not contain special characters. As of this version of vRealize Automation, the following special characters are known to cause errors:

- Double quote marks ("")
- Commas (,)
- A trailing equal sign (=)
- Blank spaces
- Non-ASCII or extended ASCII characters

Passwords that contain special characters might be accepted when you assign them, but cause failures when you perform operations such as saving endpoints or when the machine attempts to join the vRealize Automation cluster.
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.

As a best practice, all servers should be in the same domain.

The Installation Wizard runs the vRealize Automation prerequisite checker on all Windows servers before starting the installation process to ensure that the servers meet all necessary configurations.

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.
- Configure SQL Server on port 1433, the default. Do not use a non-default port.
- 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 130.

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 “Port Requirements,” on page 24.

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

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>
<thead>
<tr>
<th>Area</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Configuration</strong></td>
<td>The following components must be installed on the host before installing IaaS:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft .NET Framework 4.5.2 or later.</td>
</tr>
<tr>
<td></td>
<td>- Microsoft PowerShell 2.0 (included with Windows Server 2008 R2 SP1 and later) or Microsoft PowerShell 3.0 on Windows Server 2012 R2.</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Internet Information Services 7.5.</td>
</tr>
<tr>
<td></td>
<td>- Java must be installed on the machine running the primary Web component to support deployment of the MS SQL database during installation.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Database Requirements</strong></td>
<td>The Microsoft SQL database can reside on the IaaS (Windows) server host or on a remote host.</td>
</tr>
<tr>
<td></td>
<td>These Java-related requirements apply for databases on the IaaS (Windows) server host. They do not apply for external databases.</td>
</tr>
<tr>
<td></td>
<td>- A 64-bit version of Java 1.7 or later must be installed. 32-bit versions are not supported.</td>
</tr>
<tr>
<td></td>
<td>- The JAVA_HOME environment variable must be set to the Java installation folder.</td>
</tr>
<tr>
<td></td>
<td>- The %JAVA_HOME%\bin\java.exe file must be available.</td>
</tr>
</tbody>
</table>

**Microsoft Internet Information Services Requirements**

Your Microsoft Internet Information Services (IIS) must meet the following configuration requirements.

<table>
<thead>
<tr>
<th>IIS Component</th>
<th>Setting</th>
</tr>
</thead>
</table>
| Internet Information Services (IIS) modules installed |   - WindowsAuthentication  
   - StaticContent  
   - DefaultDocument  
   - ASP.NET 4.5  
   - ISAPIExtensions  
   - ISAPIFilter |
| IIS Authentication settings |   - 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 |   - 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.
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 or Microsoft PowerShell 3.0. PowerShell 2.0 is included with Windows Server 2008 R2 SP1 and later. Microsoft PowerShell 3.0 runs on Windows Server 2012 R2.
- SecondaryLogOnService is running.
- No firewalls can exist between DEM host and Windows Server. For port information, see “Port Requirements,” on page 24.

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

Amazon Web Services EC2 Requirements

The IaaS Windows server communicates with and collects data from an Amazon EC2 account.

When you use Amazon Web Services for provisioning, the servers that host the DEM workers must meet the following configuration requirements.

- Hosts on which DEMs are installed must have access to the Internet.
  
  If there is a firewall, HTTPS traffic must be allowed to and from aws.amazon.com, as well as the URLs representing all the EC2 regions your AWS accounts have access to, for example ec2.us-east-1.amazonaws.com for the US East region. Each URL resolves to a range of IP addresses, so you may need to use a tool, such as the one available from the Network Solutions Web site, to list and configure these IP addresses.

- Internet access from the DEM host is through a proxy server, the DEM service must be running under credentials that can authenticate to the proxy server.

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**

Any DEM worker used to manage virtual machines through SCVMM must be installed on a host on which the SCVMM console is already installed.

In addition, the following requirements must be met:

- The DEM must have access to the SCVMM PowerShell module installed with the console.
- The 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:
  
  help about_signing
  help Set-ExecutionPolicy

- If all DEM Workers within the instance are not on compute resources meeting these requirements, Skills must be used to direct all SCVMM-related workflows to those that are.

The following additional requirements apply to SCVMM.

- You must install the SCVMM console before you install 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:

  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 address this, 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. These 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 4.5.1 or later must be installed and Windows Management Instrumentation (WMI) must be enabled.

- To provision machines on an SCVMM compute resource, a user must be added in at least one security role within the SCVMM instance.

**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 open on the system. Because open, unsecure ports can be sources of security vulnerabilities, review all open ports on your system and ensure that only the ports that are required by your business applications are open.

**vRealize Automation Appliance**

The following ports are used by the vRealize Automation appliance.
Table 2-4. Incoming Ports for the vRealize Automation appliance

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Optional. SSH.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Optional. Redirects to 443.</td>
</tr>
<tr>
<td>111</td>
<td>TCP, UDP</td>
<td>RPC</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Access to the vRealize Automation console and API calls.</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Access to virtual appliance Web management interface</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Used by Management Agent</td>
</tr>
<tr>
<td>5488, 5489</td>
<td>TCP</td>
<td>Internal. Used by vRealize Automation appliance for updates.</td>
</tr>
<tr>
<td>4369, 25672,5671,5672</td>
<td>TCP</td>
<td>RabbitMQ messaging</td>
</tr>
<tr>
<td>8230, 8280, 8281</td>
<td>TCP</td>
<td>Internal vRealize Orchestrator instance</td>
</tr>
<tr>
<td>8444</td>
<td>TCP</td>
<td>Console proxy communication for vSphere VMware Remote Console connections</td>
</tr>
</tbody>
</table>

Table 2-5. Outgoing Ports for the vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>25, 587</td>
<td>TCP, UDP</td>
<td>SMTP for sending outbound notification emails</td>
</tr>
<tr>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>67, 68, 546, 547</td>
<td>TCP, UDP</td>
<td>DHCP</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Optional. For fetching software updates. Updates can be downloaded separately and applied.</td>
</tr>
<tr>
<td>110, 995</td>
<td>TCP, UDP</td>
<td>POP for receiving inbound notification emails</td>
</tr>
<tr>
<td>143, 993</td>
<td>TCP, UDP</td>
<td>IMAP for receiving inbound notification emails</td>
</tr>
<tr>
<td>123</td>
<td>TCP, UDP</td>
<td>Optional. For connecting directly to NTP instead of using host time.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>IaaS Manager Service over HTTPS Communication with virtualization hosts over HTTPS</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>ESXi network file copy operations and VMware Remote Console (VMRC) connections</td>
</tr>
<tr>
<td>5432</td>
<td>TCP, UDP</td>
<td>Optional. For communicating with an Appliance Database.</td>
</tr>
<tr>
<td>7444</td>
<td>TCP</td>
<td>Communication with SSO service over HTTPS</td>
</tr>
<tr>
<td>8281</td>
<td>TCP</td>
<td>Optional. For communicating with an external vRealize Orchestrator instance.</td>
</tr>
</tbody>
</table>

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 2.6. Incoming Ports for Infrastructure as a Service Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server instance</td>
<td>1433</td>
<td>TCP</td>
<td>MSSQL</td>
</tr>
<tr>
<td>Manager Service</td>
<td>443*</td>
<td>TCP</td>
<td>Communication with IaaS components and vRealize Automation appliance over HTTPS</td>
</tr>
<tr>
<td>vRealize Automation appliance</td>
<td>443</td>
<td>TCP</td>
<td>Communication with IaaS components and vRealize Automation appliance over HTTPS</td>
</tr>
</tbody>
</table>

* Any virtualization hosts managed by proxy agents must also have TCP port 443 open for incoming traffic.

### Table 2.7. Outgoing Ports for Infrastructure as a Service Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>All</td>
<td>67, 68, 546, 547</td>
<td>TCP, UDP</td>
<td>DHCP</td>
</tr>
<tr>
<td>All</td>
<td>123</td>
<td>TCP, UDP</td>
<td>Optional. NTP.</td>
</tr>
<tr>
<td>Manager Service</td>
<td>443</td>
<td>TCP</td>
<td>Communication with vRealize Automation appliance over HTTPS</td>
</tr>
<tr>
<td>Website</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS</td>
</tr>
<tr>
<td>Distributed Execution Managers</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS</td>
</tr>
<tr>
<td>Proxy agents</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service and virtualization hosts over HTTPS</td>
</tr>
<tr>
<td>Guest agent</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS</td>
</tr>
<tr>
<td>Manager Service, Website</td>
<td>1433</td>
<td>TCP</td>
<td>MSSQL</td>
</tr>
</tbody>
</table>

### 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 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 59.

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, supportability, and trust requirements for certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/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 2-8. Certificate Implementations

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimal Deployment (non-production)</th>
<th>Distributed Deployment (production-ready)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation Appliance</td>
<td>Generate a self-signed certificate during appliance configuration.</td>
<td>For each appliance cluster, you can use a certificate from an internal or external certificate authority. Multi-use and wildcard certificates are supported.</td>
</tr>
<tr>
<td>IaaS Components</td>
<td>During installation, accept the generated self-signed certificates or select certificate suppression.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 2-9. Sample Certificate Values and Commands (openssl)

<table>
<thead>
<tr>
<th>Certificate Authority Provides</th>
<th>Command</th>
<th>Virtual Appliance Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Private Key</td>
<td>openssl pkcs12 -in path_to_.pfx certificate_file -nocerts -out key.pem</td>
<td>RSA Private Key</td>
</tr>
<tr>
<td>PEM File</td>
<td>openssl pkcs12 -in path_to_.pfx certificate_file -clcerts -nokeys -out cert.pem</td>
<td>Certificate Chain</td>
</tr>
<tr>
<td>(Optional) Pass Phrase</td>
<td>n/a</td>
<td>Pass Phrase</td>
</tr>
</tbody>
</table>

### 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 Windows servers, consult Timekeeping best practices for Windows, including NTP.
Installing vRealize Automation with
the Installation Wizard

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

Before you begin the wizard, you must deploy a vRealize Automation appliance, configure your Windows servers to meet installation prerequisites, and verify that each appliance and server uses the same timekeeping method.

Wizard Navigation

The Installation Wizard appears the first time you log in to your vRealize Automation appliance. If you want to stop the wizard and return later, log out with the Logout button that appears on each screen. Use the Cancel button to exit the wizard and install through the management console. The wizard is disabled when you click Cancel, or when you log out of the wizard and begin an installation through the management console.

Use the Previous and Next buttons to navigate through wizard screens.

This chapter includes the following topics:
- “Deploy the vRealize Automation Appliance,” on page 31
- “Installing a Minimal Deployment with the Installation Wizard,” on page 32
- “Installing an Enterprise Deployment with the Installation Wizard,” on page 40

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. See “Password Considerations,” on page 20.

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.

- Enter the root password to use when you log in to the virtual appliance console in the Enter password and Confirm password text boxes.

- 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.

- Enter the fully qualified domain name of the virtual machine in the Hostname text box, even if you are using DHCP.

- Configure the networking properties.

11 Click Next.

12 Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.

- If Power on after deployment is available on the Ready to Complete page.
  
  a Select Power on after deployment and click Finish.
  
  b Click Close after the file finishes deploying into vCenter.
  
  c Wait for the machine to start.

  This could take up to 5 minutes.

- If Power on after deployment is not available on the Ready to Complete page.
  
  a Click Close after the file finishes deploying into vCenter.
  
  b Power on the VM and wait for some time for the VM to start up.
  
  c Verify that you can ping the DNS of the virtual machine. If you cannot ping the DNS, restart the virtual machine.

  d Wait for the machine to start. This could 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.

## Installing a Minimal Deployment with the Installation Wizard
Run the Installation Wizard for a Minimal Deployment

Install a minimal deployment for proof-of-concept work. The wizard for minimal installation assumes you are installing all IaaS components on a single Windows machine.

Minimal deployments typically support a single vRealize Automation appliance, an IaaS server, and use a vSphere agent to support endpoints.

Prerequisites

- Verify that you have met the prerequisites described in Chapter 2, “Preparing for Installation,” on page 19
- “Deploy the vRealize Automation Appliance,” on page 61

Procedure

1. Open a Web browser.
3. Log in with the user name root and the password you specified when the appliance was deployed.
4. When the Installation Wizard appears, click Next.
5. Accept the End User License Agreement and click Next.
6. Select Minimal Deployment and Install Infrastructure as a Service on the Deployment Type screen and click Next.
7. Check that the prerequisites listed on the Installation Prerequisites page have been met and that the Windows servers on which you installed a Management Agent are listed.
8. If needed, you can change the timekeeping method for your vRealize Automation appliance. Click Change Time Settings, if you make changes.
9. Click Next.
10. Click Run on the Run the Prerequisite Checker screen to verify that the Windows servers in your deployment are correctly configured for vRealize Automation use.
    Because this step runs remotely, it can take several minutes for the step to run.
    a. If a failed status is returned for a machine, click Fix to start automatic corrections or click Show Details and follow the instructions. Automatic corrections also restart
    b. Click Run to rerun the checker.
    c. When all statuses show success, click Next.
11. Proceed through the next screens, supplying the requested information to configure your deployment components, including the Web server, Manager Service, Distributed Execution Manager, vSphere proxy agent, and certificate information.

What to do next

“Create Snapshots Before You Begin the Installation,” on page 37
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 34
   When you install a management agent, you must validate the fingerprint of the SSL certificate for the Management Site service.

2. **Download and Install a Management Agent** on page 34
   An administrator downloads and installs a Management Agent on IaaS machines in your deployment. The Management Agent must be installed on all IaaS servers except for those that are used exclusively for your MS SQL database.

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:

   ```
   ```

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 a Management Agent

An administrator downloads and installs a Management Agent on IaaS machines in your deployment. The Management Agent must be installed on all IaaS servers except for those that are used exclusively for your MS SQL database.

The Management Agent registers IaaS nodes 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 on your IaaS machine and you must have local administrator rights to install the agent.

Prerequisites

- “Find the SSL Certificate Fingerprint for the Management Site Service,” on page 34
- Verify that the service account user, or domain user, is part of the local administrators group of each IaaS machine.
Procedure

1. Open your vRealize Automation appliance by specifying an address of the following form in a Web browser, where `vra-va-hostname.domain.name` is the fully qualified domain name of your vRealize Automation appliance. Do not use a load balancer address.

   https://vra-va-hostname.domain.name:5480/installer

2. Click **Management Agent installer** to download the installer.

3. Run the Management Agent installer, vCAC-IaaSManagementAgent-Setup.msi.

   The default installation location is `%Program Files(x86)%\VMware\vCAC\Management Agent\`

4. Click **Next** on the Welcome page.

5. Accept the EULA and click **Next**.

6. Provide an alternative installation path or accept the default value.

7. Click **Next**.

8. Enter the Management Site Service details for the following fields. and click **Next**.

<table>
<thead>
<tr>
<th>Text box</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vRA appliance address</strong></td>
<td><a href="https://vra-va-hostname.domain.name:5480">https://vra-va-hostname.domain.name:5480</a></td>
</tr>
<tr>
<td>You must specify the port number.</td>
<td></td>
</tr>
<tr>
<td><strong>Root username</strong></td>
<td>The root user for the vRealize Automation appliance.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The root user password for the vRealize Automation appliance.</td>
</tr>
<tr>
<td><strong>Management Site server certificate</strong></td>
<td>The SHA1 fingerprint for the Management Site Service certificate. The Management Site Service is hosted on the vRealize Automation appliance. Sample SHA1 fingerprint: DFF5FA0886DA2920D227ADFD880C9CDE4EF13EEF78.</td>
</tr>
<tr>
<td><strong>Load</strong></td>
<td>Click <strong>Load</strong> to load the default fingerprint.</td>
</tr>
</tbody>
</table>

Management Site Service

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

- **vRA appliance address**: https://vra-address:5480/
- **Root username**: root
- **Password**: ********
- **Management Site Service certificate SHA1 fingerprint**: 8F03EF5813D4E35B2F6C77062B1C241D10E882
- **I confirm the fingerprint matches the Management Site Service SSL certificate**: 

---

VMware, Inc.  35
9  Select the **Fingerprint match confirmation** checkbox after you confirm that the fingerprint that is displayed matches the fingerprint of the Management Site SSL certificate.

   If the fingerprints do not match, check that the address in the **vRA appliance address** text box is correct.

10  Click **Next**.

11  Enter the service account user name and password.

12  Click **Next**.

13  Click **Install**.

14  Click **Finish**.

15  Repeat these steps for each Windows IaaS host.

After you installed the Management Agent, the Windows server is listed 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Time Server</strong></td>
<td>Select <strong>Use Time Server</strong> from the <strong>Time Sync Mode</strong> menu to use Network Time Protocol. For each time server that you are using, enter the IP address or the host name in the <strong>Time Server</strong> text box.</td>
</tr>
<tr>
<td><strong>Use Host Time</strong></td>
<td>Select <strong>Use Host Time</strong> from the <strong>Time Sync Mode</strong> 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.</td>
</tr>
</tbody>
</table>

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 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. This also restarts the Windows machine as needed.
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 Deployment Configuration Parameters**
Specify configuration parameters for your deployment components.

**Prerequisites**

**Procedure**
1 On the vRealize Automation Host screen, specify the host.
   - Click Resolve Automatically to have vRealize Automation supply the default address.
   - Click Enter Host and enter the DNS alias or FQDN for a different host.
2 Click Next.
3 On the Single Sign-on screen, enter the password for the system administrator for the default tenant account and confirm the password by re-entering it.
4 Click Next.
5 Continue through the following screens, using the context sensitive help if you need additional information.
6 Click Next after you complete the Validation screen.

**What to do next**
Create a snapshot of your machines before you begin the 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 in 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 57

**Scenario: Finish the Installation**

As the vSphere administrator, you are at the last part of the installation process. 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 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 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 into 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 Chapter 5, “Configure Access to the Default Tenant,” on page 113.
Installing an Enterprise Deployment with the Installation Wizard

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 Installation,” on page 19
- “Deploy the vRealize Automation Appliance,” on page 61.

Procedure

1. Open a Web browser.
3. Log in with the user name root and the password you specified when the appliance was deployed.
4. The Installation Wizard appears the first time you log in to the appliance.
5. Accept the End User License Agreement and click Next.
6. Select Enterprise deployment and Install Infrastructure as a Service on the Deployment Type screen and click Next.
7. Check that the prerequisites listed on the Installation Prerequisites page have been met and that the Windows servers on which you installed a Management Agent are listed.
8. If needed, you can change the timekeeping method for your vRealize Automation appliance. Click Change Time Settings, if you make changes.
9. Click Next.

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:
   ```
   ```
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 a Management Agent

An administrator downloads and installs a Management Agent on IaaS machines in your deployment. The Management Agent must be installed on all IaaS servers except for those that are used exclusively for your MS SQL database.

The Management Agent registers IaaS nodes 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 on your IaaS machine and you must have local administrator rights to install the agent.

Prerequisites

- “Find the SSL Certificate Fingerprint for the Management Site Service,” on page 34
- Verify that the service account user, or domain user, is part of the local administrators group of each IaaS machine.

Procedure

1. Open your vRealize Automation appliance by specifying an address of the following form in a Web browser, where `vra-va-hostname.domain.name` is the fully qualified domain name of your vRealize Automation appliance. Do not use a load balancer address.
   ```
   https://vra-va-hostname.domain.name:5480/installer
   ```
2. Click **Management Agent installer** to download the installer.
3. Run the Management Agent installer, vCAC-IaaSManagementAgent-Setup.msi.
   The default installation location is `%Program Files(x86)%\VMware\vCAC\Management Agent\`
4. Click **Next** on the Welcome page.
5. Accept the EULA and click **Next**.
6. Provide an alternative installation path or accept the default value.
7. Click **Next**.
8 Enter the Management Site Service details for the following fields. and click Next.

<table>
<thead>
<tr>
<th>Text box</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRA appliance address</td>
<td><a href="https://vra-va-hostname.domain.name:5480">https://vra-va-hostname.domain.name:5480</a></td>
</tr>
<tr>
<td></td>
<td>You must specify the port number.</td>
</tr>
<tr>
<td>Root username</td>
<td>The root user for the vRealize Automation appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>The root user password for the vRealize Automation appliance.</td>
</tr>
<tr>
<td>Management Site server certificate</td>
<td>The SHA1 fingerprint for the Management Site Service certificate. The Management Site Service is hosted on the vRealize Automation appliance. Sample SHA1 fingerprint: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.</td>
</tr>
<tr>
<td>Load</td>
<td>Click Load to load the default fingerprint.</td>
</tr>
</tbody>
</table>

9 Select the Fingerprint match confirmation checkbox after you confirm that the fingerprint that is displayed matches the fingerprint of the Management Site SSL certificate.

If the fingerprints do not match, check that the address in the vRA appliance address text box is correct.

10 Click Next.

11 Enter the service account user name and password.

12 Click Next.

13 Click Install.

14 Click Finish.

15 Repeat these steps for each Windows IaaS host.

After you installed the Management Agent, the Windows server is listed 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Time Server</td>
<td>Select <em>Use Time Server</em> from the <em>Time Sync Mode</em> menu to use Network Time Protocol. For each time server that you are using, enter the IP address or the host name in the <em>Time Server</em> text box.</td>
</tr>
<tr>
<td>Use Host Time</td>
<td>Select <em>Use Host Time</em> from the <em>Time Sync Mode</em> 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.</td>
</tr>
</tbody>
</table>

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. This also restarts the Windows machine as needed.

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 Deployment Configuration Parameters

Specify configuration parameters for your deployment components.

Prerequisites

Procedure

1. On the vRealize Automation Host screen, specify the host.
   - Click Resolve Automatically to have vRealize Automation supply the default address.
   - Click Enter Host and enter the DNS alias or FQDN for a different host.
2. Click Next.
3. On the Single Sign-on screen, enter the password for the system administrator for the default tenant account and confirm the password by re-entering it.
4. Click Next.
5. Continue through the following screens, using the context sensitive help if you need additional information.
6. Click Next after you complete the Validation screen.

What to do next

Create snapshots of your machines before you begin the 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.

\[\text{Note} \quad \text{Do not exit the installation wizard or cancel the installation.}\]

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 57
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 into 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 Chapter 5, “Configure Access to the Default Tenant,” on page 113.
Installing vRealize Automation through the Standard Interfaces

As an alternative to the Installation Wizard, you can install vRealize Automation through the vRealize Automation appliance management console and the IaaS manual installer.

Installation through the standard interface is intended primarily for

This chapter includes the following topics:

- “Minimal Deployment,” on page 47
- “Distributed Deployment,” on page 57
- “Installing Agents,” on page 91

Minimal Deployment

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan and prepare the installation environment and verify that all installation prerequisites are met.</td>
<td>Chapter 2, “Preparing for Installation,” on page 19</td>
</tr>
<tr>
<td>Set up your vRealize Automation appliance</td>
<td>“Deploy and Configure the vRealize Automation Appliance,” on page 48</td>
</tr>
<tr>
<td>Install IaaS components on a single Windows server.</td>
<td>“Installing IaaS Components,” on page 52</td>
</tr>
<tr>
<td>Install additional agents, if required.</td>
<td>&quot;Installing Agents,&quot; on page 91</td>
</tr>
<tr>
<td>Perform post-installation tasks such as configuring the default tenant.</td>
<td></td>
</tr>
</tbody>
</table>
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 48
   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 49
   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 50
   To prepare the vRealize Automation appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides 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. See “Password Considerations,” on page 20.

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, even if you are using DHCP.
   d Configure the networking properties.
11 Click Next.
12 Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.
   ■ If Power on after deployment is available on the Ready to Complete page.
      a Select Power on after deployment and click Finish.
      b Click Close after the file finishes deploying into vCenter.
      c Wait for the machine to start.
      This could take up to 5 minutes.
   ■ If Power on after deployment is not available on the Ready to Complete page.
      a Click Close after the file finishes deploying into vCenter.
      b Power on the VM and wait for some time for the VM to start up.
      c Verify that you can ping the DNS of the virtual machine. If you cannot ping the DNS, restart the virtual machine.
      d Wait for the machine to start. This could 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

Procedure
1 Navigate to the vRealize Automation appliance management console by using its fully qualified domain name, https://vra-va-hostname.domain.name:5480/.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Time Server</strong></td>
<td>Select Use Time Server from the <strong>Time Sync Mode</strong> menu to use Network Time Protocol. For each time server that you are using, enter the IP address or the host name in the <strong>Time Server</strong> text box.</td>
</tr>
<tr>
<td><strong>Use Host Time</strong></td>
<td>Select Use Host Time from the <strong>Time Sync Mode</strong> 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.</td>
</tr>
</tbody>
</table>

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, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

**Prerequisites**

“Enable Time Synchronization on the vRealize Automation Appliance,” on page 49.

**Procedure**

1 Navigate to the vRealize Automation appliance management console by using its fully qualified domain name, https://vra-va-hostname.domain.name:5480/.

2 Continue past the certificate warning.

3 Log in with user name root and the password you specified when you deployed vRealize Automation appliance.

4 Select **vRA Settings > Host Settings**.

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

**Note** Configure SSO settings as described later in this procedure whenever you use **Update Host** to change a host name.
6 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**

- 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**

- 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.

7 Click Save Settings to save host information and SSL configuration.

8 Configure the SSO settings.

9 Click Messaging. The configuration settings and status of messaging for your appliance is displayed. Do not change these settings.

10 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](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.
11 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.

12 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.

13 Confirm that you can log in to the vRealize Automation console.
   a Open a browser and navigate to `https://vcac-hostname.domain.name/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 console 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**

“Install the Infrastructure Components,” on page 53

### 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 71 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 21.
- 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 IaaS Installer** on page 54
   A system administrator downloads the installer to a Windows 2008 or Windows 2012 physical or virtual machine.

2 **Select the Installation Type** on page 54
   The system administrator runs the installer wizard from the Windows 2008 or 2012 installation machine.

3 **Check Prerequisites** on page 55
   The Prerequisite Checker verifies that your machine meets IaaS installation requirements.

4 **Specify Server and Account Settings** on page 55
   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 56
   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 56
   The system administrator installs the IaaS certificate and registers the IaaS components with the SSO.

7 **Finish the Installation** on page 57
   The system administrator finishes the IaaS installation.
Download the IaaS Installer

A system administrator downloads the installer to a Windows 2008 or Windows 2012 physical or virtual machine.

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

Prerequisites

- Microsoft .NET Framework 4.5.1 or later must be installed on the IaaS installation machine. You can download the .NET installer from the installer Web page.

- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. See res://iesetup.dll/SoftAdmin.htm.

- Log in to the Windows server as a local administrator.

Procedure

1. Log in to the Windows machine where you are about to perform the installation.
2. Open a Web browser.
3. Enter the URL of the VMware vRealize Automation IaaS Installation download page.
   For example, https://vra-va-hostname.domain.name:5480/installer, where vra-va-hostname.domain.name is the name of the vRealize Automation appliance host.
4. Download the installer by clicking on the IaaS Installer link.
5. When prompted, save the installer file, setup__vra-va-hostname.domain.name@5480, to the desktop.
   Do not change the 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 IaaS Installer,” on page 71.

Procedure

1. Right-click the setup__vra-va-hostname.domain.name@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 54.

**Procedure**

1 Complete the Prerequisite Check.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No errors</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Noncritical errors</td>
<td>Click Bypass.</td>
</tr>
<tr>
<td>Critical errors</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 55.

**Procedure**

1 On the Server and Account Settings page or the Detected Settings page, specify the user name and password for a user with SQL administrative privileges or a local administrator.

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 In the **Server** text box in the SQL Server Database Installation Information section, accept the default server to install the database instance on the same server with the IaaS components, or type a different server name if the database is on another machine.

   If you specify a different server, you must supply the server name and port number, using the form `servername,portnumber`.

4 Accept the default in the **Database name** text box or type an 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.

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 related information about configuring SSL on the SQL server, see KB article 316898 *How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console* at the Microsoft support site.

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 55.

**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 IaaS Installer,” on page 54.

**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 56.
- 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 90.

**Distributed Deployment**

In a distributed 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Plan and prepare the installation environment and verify that all installation prerequisites are met.</td>
<td>Chapter 2, “Preparing for Installation,” on page 19</td>
</tr>
<tr>
<td>☐ Plan for and obtain your SSL certificates.</td>
<td>“Certificate Trust Requirements in a Distributed Deployment,” on page 59</td>
</tr>
<tr>
<td>☐ Deploy the lead vRealize Automation appliance server, and any additional appliances you require for redundancy and high availability.</td>
<td>“Deploy the vRealize Automation Appliance,” on page 61</td>
</tr>
<tr>
<td>☐ Configure your load balancer to handle vRealize Automation appliance traffic.</td>
<td>“Configuring Appliances for vRealize Automation,” on page 63</td>
</tr>
<tr>
<td>☐ Configure your load balancer to handle the vRealize Automation IaaS component traffic and install vRealize Automation IaaS components.</td>
<td>“Install the IaaS Components in a Distributed Configuration,” on page 69</td>
</tr>
<tr>
<td>☐ If required, install agents to integrate with external systems.</td>
<td>“Installing Agents,” on page 91</td>
</tr>
<tr>
<td>☐ Configure the default tenant and provide the IaaS license.</td>
<td></td>
</tr>
</tbody>
</table>

vRealize Orchestrator

Use external implementations of vRealize Orchestrator with high-availability deployments. If you use a vRealize Orchestrator server on a vRealize Automation appliance, configure it to be external. Embedded versions should never be used.

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 Configuring vRealize Automation.

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>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.</td>
</tr>
<tr>
<td>Appliance Database</td>
<td>Stores information required by the virtual appliances. The database is embedded on one or two instances of vRealize Automation appliance.</td>
</tr>
</tbody>
</table>

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

Table 4-4. IaaS Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>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.</td>
</tr>
<tr>
<td>Manager Service</td>
<td>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.</td>
</tr>
<tr>
<td>Model Manager</td>
<td>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.</td>
</tr>
<tr>
<td>Distributed Execution Managers (Orchestrator and Worker)</td>
<td>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.</td>
</tr>
<tr>
<td>Agents</td>
<td>Virtualization, integration, and WMI agents that communicate with infrastructure resources.</td>
</tr>
</tbody>
</table>

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 multi-use certificate that includes the IaaS Web component in the cluster, and then copy that multi-use certificate to each component in the cluster. You can use Subject Alternative Name (SAN) certificates, wildcard certificates, or any other method of multi-use certification appropriate for your environment as long as you satisfy the trust requirements. Depending on your load balancer configuration, you may need to certify the load balancer as part of the multi-use certificate for the cluster.
For example, if you have a load balancer configuration that requires a certificate on the load balancer as well as its components, you might obtain a SAN certificate to certify web-load-balancer.eng.mycompany.com, web-component-1.eng.mycompany.com, and web-component-2.eng.mycompany.com. You would copy that single multi-use certificate to the load balancer and each of the appliances and then register the certificate on the Web component machines.

The Certificate Importation and Registration table summarizes the registration requirements for various imported certificates.

**Table 4-5. Certificate Importation and Registration**

<table>
<thead>
<tr>
<th>Import</th>
<th>Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance cluster</td>
<td>Web components cluster</td>
</tr>
<tr>
<td>Web components cluster</td>
<td>vRealize Automation appliance cluster</td>
</tr>
<tr>
<td>Web components cluster</td>
<td>Manager Service components cluster</td>
</tr>
<tr>
<td>Web components cluster</td>
<td>DEM Orchestrators and DEM Worker components</td>
</tr>
<tr>
<td>Manager Service components cluster</td>
<td>DEM Orchestrators and DEM Worker components</td>
</tr>
<tr>
<td></td>
<td>Agents and Proxy Agents</td>
</tr>
</tbody>
</table>

**Installation Worksheets**

You can use these worksheets to record important information for reference during the installation process. One copy of each worksheet is given here. Create additional copies as you need them. Settings are case sensitive.

**Table 4-6. Leading cluster vRealize Automation appliance Information**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (FQDN)</td>
<td>vcac-va.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>SSO service over HTTPS Outgoing Port (default)</td>
<td>7444 (do not change)</td>
<td>7444</td>
</tr>
<tr>
<td>IP</td>
<td>192.168.1.105</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> (default)</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vmware</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4-7. Additional vRealize Automation appliance Information**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (FQDN)</td>
<td>vcac-va2.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>SSO service over HTTPS Outgoing Port (default)</td>
<td>7444 (do not change)</td>
<td>7444</td>
</tr>
<tr>
<td>IP</td>
<td>192.168.1.110</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> (default)</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vmware</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4-8. IaaS Database Passphrase**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passphrase (reused in IaaS Installer, Upgrade, and Migration)</td>
<td>myPassphrase</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-9. IaaS Website

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (FQDN)</td>
<td></td>
<td>iaas-web.mycompany.com</td>
</tr>
<tr>
<td>SSO service over HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outgoing Port (default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td>192.168.1.106</td>
</tr>
<tr>
<td>Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4-10. IaaS Model Manager Data

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (FQDN)</td>
<td></td>
<td>iaas-model-man.mycompany.com</td>
</tr>
<tr>
<td>SSO service over HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outgoing Port (default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td>192.168.1.107</td>
</tr>
<tr>
<td>Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4-11. IaaS Model Service

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (FQDN)</td>
<td></td>
<td>iaas-model-service.mycompany.com</td>
</tr>
<tr>
<td>SSO service over HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outgoing Port (default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td>192.168.1.108</td>
</tr>
<tr>
<td>Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4-12. Distributed Execution Managers

<table>
<thead>
<tr>
<th>Unique Name</th>
<th>Orchestrator/Worker</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex. myuniqueorchestratorname</td>
<td>Orchestrator:</td>
</tr>
<tr>
<td></td>
<td>Worker:</td>
</tr>
<tr>
<td></td>
<td>Orchestrator:</td>
</tr>
<tr>
<td></td>
<td>Worker:</td>
</tr>
<tr>
<td></td>
<td>Orchestrator:</td>
</tr>
<tr>
<td></td>
<td>Worker:</td>
</tr>
<tr>
<td></td>
<td>Orchestrator:</td>
</tr>
<tr>
<td></td>
<td>Worker:</td>
</tr>
</tbody>
</table>

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. See “Password Considerations,” on page 20.
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, even if you are using DHCP.
    d. Configure the networking properties.
11. Click Next.
12. Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.
    a. If Power on after deployment is available on the Ready to Complete page.
       a. Select Power on after deployment and click Finish.
       b. Click Close after the file finishes deploying into vCenter.
       c. Wait for the machine to start.
       This could take up to 5 minutes.
    b. If Power on after deployment is not available on the Ready to Complete page.
       a. Click Close after the file finishes deploying into vCenter.
       b. Power on the VM and wait for some time for the VM to start up.
       c. Verify that you can ping the DNS of the virtual machine. If you cannot ping the DNS, restart the virtual machine.
Wait for the machine to start. This could 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 59. For information about extracting certificates, see “Extracting Certificates and Private Keys,” on page 28.
5. Configure the load balancer for vRealize Automation appliance traffic.

**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 VMware vRealize Automation Reference Architecture, available as a technical paper at https://www.vmware.com/support/pubs/vcac-pubs.html.

**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 61.
- Get a domain certificate for the vRealize Automation appliance.
Procedure

1. **Enable Time Synchronization on the vRealize Automation appliance** on page 64
   
   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 64
   
   To prepare the vRealize Automation appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides 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**


2. Log in with the user name `root` and the password you specified when the appliance was deployed.


4. Select an option from the `Time Sync Mode` menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Time Server</td>
<td>Select <strong>Use Time Server</strong> from the <code>Time Sync Mode</code> 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.</td>
</tr>
<tr>
<td>Use Host Time</td>
<td>Select <strong>Use Host Time</strong> from the <code>Time Sync Mode</code> 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.</td>
</tr>
</tbody>
</table>

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, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

**Procedure**


2. Continue past the certificate warning.

3. Log in with user name root and the password you specified when you deployed vRealize Automation appliance.
4 Select vRA Settings > Host Settings.

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

**NOTE** Configure SSO settings as described later in this procedure whenever you use Update Host to change a 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Existing</td>
<td>Leave the current SSL configuration. Select this option to cancel your changes.</td>
</tr>
</tbody>
</table>
| Generate Certificate | 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. |

<table>
<thead>
<tr>
<th>Import</th>
<th>Action</th>
</tr>
</thead>
</table>
| 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.  
| 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.  
| NOTE In the case of chained certificates, additional attributes may be available. |
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](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 into vRealize Automation console.

a. Open a browser and navigate to https://vcac-hostname.domain.name/vcac/.
   
   If you are using a load balancer, the host name must be the fully qualified domain name of the load balancer.

b. If prompted, continue past the certificate warnings.

b. Log in with administrator@vsphere.local and the password you specified when configuring SSO.

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

15 If you are using a load balancer and all nodes under the load balancer have been configured, configure and enable any applicable health checks.

Configuring Additional Instances of 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 63.

Procedure


2. Log in with the user name root and the password you specified when the appliance was deployed.


4. Select an option from the Time Sync Mode menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Time Server</td>
<td>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.</td>
</tr>
<tr>
<td>Use Host Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

**Join a vRealize Automation appliance to a Cluster**

Distributed installations that use load balancers support the use of more than one vRealize Automation appliance in a deployment. Each appliance in the deployment must belong to a cluster.

You join a vRealize Automation appliance to a cluster from the management console. The join operation copies appliance configuration information for the cluster to the appliance you are adding to the cluster, including certificate, SSO, licensing, database, and messaging information.

Perform this task from the management console of each server you want to join to the cluster except for the leading cluster node.

The join operation is not required for the leading cluster node because the join operation links the leading cluster node with the node from whose management console you are working, which makes both nodes part of the same cluster. After an appliance is part of the cluster, you can specify its FQDN as the leading cluster node.

**NOTE** When you add the first node to a cluster, you might need to re-import or recreate the certificate. Also, you should add nodes to a cluster one at a time and not in parallel.

**Prerequisites**

- “Configure the Primary vRealize Automation Appliance,” on page 63.
- If your site is using a load balancer, verify that it is configured for use with your vRealize Automation appliance.
- “Enable Time Synchronization on the vRealize Automation Appliance,” on page 67. Time synchronization must be enabled for each appliance.
- Verify that traffic can pass through the load balancer to the installed nodes and to the node being configured. The primary node must also be available.

**Procedure**


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.
Verify that services are running.

- Click the **Services** tab.
- Click the **Refresh** tab to monitor the progress of service startup.

**Disable Unused Services**

A system administrator can disable the embedded vRealize Orchestrator services. These services are not used in a distributed deployment so they should be disabled so as not to consume unnecessary resources.

**Prerequisites**

“Join a vRealize Automation appliance to a Cluster,” on page 68

**Procedure**

1. Log in to the vRealize Automation appliance by using SSH.
2. Stop the embedded vRealize Orchestrator service.
   ```bash
   service vco-server stop
   chkconfig vco-server off
   ```
3. Log out of the vRealize Automation appliance.

**Validate the Distributed Deployment**

After deploying additional instances of the vRealize Automation appliance, you should 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 the vRealize Automation console by navigating to `https://vcac-hostname.domain.name/vcac`, where `vcac-hostname.domain.name` is the address of the load balancer.
3. After you have verified that the new vRealize Automation appliance is accessible by using 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.

**Prerequisites**

- “Configure the Primary vRealize Automation Appliance,” on page 63.
- If your site includes multiple instances of vRealize Automation appliance, “Join a vRealize Automation appliance to a Cluster,” on page 68.
- Verify that your installation servers meet the requirements described in “IaaS Web Service and Model Manager Server Requirements,” on page 21.
- 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 71
   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 IaaS Installer** on page 71
   A system administrator downloads the IaaS installer from the vRealize Automation appliance to a Windows 2008 or Windows 2012 physical or virtual machine.

3. **Choosing an IaaS Database Scenario** on page 72
   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 77
   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 Website Components** on page 80
   The Website component provides access to infrastructure capabilities in the vRealize Automation Web console. The system administrator can install one or many instances of the Website component.

6. **Install the Active Manager Service** on page 82
   The Manager Service component coordinates communication between agents and proxy agents, the database, and SMTP. A minimum of one instance of the Manager Service component must be installed. You can install one active instance and one backup instance of the Manager Service component to provide redundancy in a high-availability deployment.

7. **Install a Backup Manager Service Component** on page 84
   You can install a passive backup instance of the Manager Service component that you can start manually to provide redundancy in a high-availability deployment.

8. **Installing Distributed Execution Managers** on page 86
   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 89
   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 90
    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 86.
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

You must disable TLS1.2 for certificates using SHA512 on Windows 2012 machines. For more information about disabling TLS1.2, consult the Microsoft Knowledge Base article at http://support.microsoft.com/kb/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 IaaS Installer,” on page 71.

Download the IaaS Installer

A system administrator downloads the IaaS installer from the vRealize Automation appliance to a Windows 2008 or Windows 2012 physical or virtual machine.

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

Prerequisites

- “Configure the Primary vRealize Automation Appliance,” on page 63 and, optionally, “Join a vRealize Automation appliance to a Cluster,” on page 68.
- Verify that your installation servers meet the requirements described in “IaaS Web Service and Model Manager Server Requirements,” on page 21.
- 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 Windows machine where you are about to perform the installation.

3. Open a Web browser.

4. Enter the URL of the VMware vRealize Automation IaaS Installation download page.
   For example, `https://vra-va-hostname.domain.name:5480/installer`, where `vra-va-hostname.domain.name` is the name of your vRealize Automation appliance host.

5. Download the installer by clicking on the **IaaS Installer** link.

6. When prompted, save the installer file, `setup_vra-va-hostname.domain.name@5480.exe`, to the desktop.
   Do not change the file name. It is used to connect the installation to the vRealize Automation appliance.

7. Download the installer file to each machine on which you are installing components.

What to do next

Install an IaaS database, see “Choosing an IaaS Database Scenario,” on page 72.

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 KB 316898 *How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console* at the Microsoft support site.
Table 4-13. Choosing an IaaS Database Scenario

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>“Create the IaaS Database Manually,” on page 73.</td>
</tr>
<tr>
<td>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.</td>
<td>“Prepare an Empty Database,” on page 74.</td>
</tr>
<tr>
<td>Use the installer to create the database. This is the simplest option but requires the use of sysadmin privileges in the installer.</td>
<td>“Create the IaaS Database Using the Installation Wizard,” on page 75.</td>
</tr>
</tbody>
</table>

Create the IaaS Database Manually

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

Prerequisites

- .NET 4.5.1 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.
- Download the IaaS database installer scripts from the vRealize Automation appliance by navigating to https://vra-va-hostname.domain.name: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.
4. 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.
5. Execute the following command with the arguments described in the table.

```batch
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 4-14. Database Values

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_server</td>
<td>Specifies the SQL Server instance in the format dbhostname[,port number]\SQL instance. 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 db_server is localhost.</td>
</tr>
<tr>
<td>db_name</td>
<td>Name of the database. The default value is vra. Database names must consist of no more than 128 ASCII characters.</td>
</tr>
<tr>
<td>db_dir</td>
<td>Path to the data directory for the database, excluding the final slash.</td>
</tr>
<tr>
<td>log_dir</td>
<td>Path to the log directory for the database, excluding the final slash.</td>
</tr>
<tr>
<td>service_user</td>
<td>User name under which the Manager Service runs.</td>
</tr>
<tr>
<td>Web_user</td>
<td>User name under which the Web services run.</td>
</tr>
<tr>
<td>version_string</td>
<td>Specifies the vRealize Automation version. For example, for version 6.1, the version string is 6.1.8.1208.</td>
</tr>
</tbody>
</table>

The database is created.

What to do next

“Install the IaaS Components in a Distributed Configuration,” on page 69.

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.
- Download the IaaS database installer scripts from the vRealize Automation appliance by navigating to https://vra-va-hostname.domain.name:5480/installer/.

Procedure

1. Navigate to the database directory within the directory where you extracted the installation zip archive.
2. Extract the DBInstal1.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 4-15. Database Values

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

Open SQL Server Management Studio.

Click New Query.

An SQL Query window opens.

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

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

Click Execute.

The script runs and creates the database.

What to do next

"Install the IaaS Components in a Distributed Configuration," on page 69.

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 73.

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 IaaS Installer,” on page 71.

Procedure

1 Right-click the setup__vra–va–hostname.domain.name@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.

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 configure SSL on the SQL server to support this option. For related information about configuring SSL on the SQL server, see KB article 316898 How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console at the Microsoft support site.

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.

16 Click Next.

17 Complete the Prerequisite Check.

\[
\begin{array}{|c|c|}
\hline
\text{Option} & \text{Description} \\
\hline
\text{No errors} & \text{Click Next.} \\
\hline
\text{Noncritical errors} & \text{Click Bypass.} \\
\hline
\text{Critical errors} & \text{Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click Check Again to verify.} \\
\hline
\end{array}
\]

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 72.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “Security Passphrase,” on page 29.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1. **Install the First IaaS Website Component** on page 77
   
   A system administrator installs a Website component to provide access to infrastructure capabilities on the vRealize Automation Web console.

2. **Configure Model Manager Data** on page 78
   
   You install the Model Manager component on the same machine that hosts the first Website component. You can only install Model Manager Data once.

You can install additional Website components or install the Manager Service. See “Install Additional IaaS Website Components,” on page 80 or “Install the Active Manager Service,” on page 82.

Install the First IaaS Website Component

A system administrator installs a Website component to provide access to infrastructure capabilities on the vRealize Automation Web console.

You can install multiple Website components, but only one can contain Model Manager Data. Model Manager Data should be installed on the first Website component you create.

Prerequisites

- “Create the IaaS Database Using the Installation Wizard,” on page 75.
- Verify that your environment meets the requirements described in “IaaS Web Service and Model Manager Server Requirements,” on page 21.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “Security Passphrase,” on page 29.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1. Disable any health checks for the load balancer and ensure that traffic is directed to the node.
2. Disable any other nodes under the load balancer.
3. Right-click the setup__vra–hostname.domain.name@5480.exe setup file and select **Run as administrator**.
4. Click Next.
5. Accept the license agreement and click **Next**.
6 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.

7 Click Next.

8 Select Custom Install on the Installation Type page.

9 Select IaaS Server under Component Selection on the Installation Type page.

10 Accept the root install location or click Change and select an installation path.

11 Click Next.

12 Select Website and ModelManagerData on the IaaS Server Custom Install page.

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 (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 Website component. You can only install Model Manager Data once.

Prerequisites

"Install the First IaaS Website Component," on page 77.

Procedure

1 Click the Model Manager Data tab.
2 Type the fully qualified domain name of the vRealize Automation appliance in the Server text box.
   IP addresses are not recognized.
   For example, vra.mycompany.com.

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 Type the fully qualified name of the IaaS Website server in the IaaS Server text box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, IaaS-load-balancer.eng.mycompany.com. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Type the fully qualified domain name of the IaaS Website Server. For example, IaaS.eng.mycompany.com. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

10 Click Test to verify the server connection.

11 Click Next.

12 Complete the Prerequisite Check.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No errors</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Noncritical errors</td>
<td>Click Bypass.</td>
</tr>
<tr>
<td>Critical errors</td>
<td>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.</td>
</tr>
</tbody>
</table>

13 Type the user name and password of the service account user who has administrative privileges on the current installation server in the Server Installation Information text boxes on the Server and Account Settings page.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have already installed components in this environment</td>
<td>Type the passphrase you created previously in the Passphrase and Confirm text boxes.</td>
</tr>
<tr>
<td>If this is the first installation</td>
<td>Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.</td>
</tr>
</tbody>
</table>

Keep this passphrase in a secure place for later use.
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.

Click Next.

Click Install.

When the installation finishes, deselect Guide me through the initial configuration and click Next.

What to do next

You can install additional Website components or install the Manager Service. See “Install Additional IaaS Website Components,” on page 80 or “Install the Active Manager Service,” on page 82. If you do not plan to add more nodes under the load balancer, enable any applicable health checks.

Install Additional IaaS Website Components

The Website component provides access to infrastructure capabilities in the vRealize Automation Web console. The system administrator can install one or many instances of the Website component.

Do not install Model Manager Data with the Website component. Only the first Website component you install can contain Model Manager Data.

Prerequisites

- “Install an IaaS Website Component and Model Manager Data,” on page 77.
- Verify that your environment meets the requirements described in “IaaS Web Service and Model Manager Server Requirements,” on page 21.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “Security Passphrase,” on page 29.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1. Disable any health checks for the load balancer and ensure that traffic is directed to the node.
2. Right-click the setup__vra-va-hostname.domain.name@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.

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 Type IaaS server information in the **IaaS Server** text box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, <em>IaaS-load-balancer.eng.mycompany.com</em>.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Type the fully qualified domain name of the IaaS Website Server. For example, <em>IaaS.eng.mycompany.com</em>.</td>
</tr>
</tbody>
</table>

19 Click **Test** to verify the server connection.

20 Click **Next**.

21 Complete the Prerequisite Check.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No errors</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Noncritical errors</td>
<td>Click <strong>Bypass</strong>.</td>
</tr>
<tr>
<td>Critical errors</td>
<td>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 <strong>Check Again</strong> to verify.</td>
</tr>
</tbody>
</table>

22 Type the user name and password of the service account user who has administrative privileges on the current installation server in the **Server Installation Information** text boxes on the Server and Account Settings page.
23 Provide the passphrase used to generate the encryption key that protects the database.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have already installed components in this environment</td>
<td>Type the passphrase you created previously in the Passphrase and Confirm text boxes.</td>
</tr>
<tr>
<td>If this is the first installation</td>
<td>Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.</td>
</tr>
</tbody>
</table>

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 82. If you do not plan to add more nodes under the load balancer, enable any applicable health checks.

Install the Active Manager Service

The Manager Service component coordinates communication between agents and proxy agents, the database, and SMTP. A minimum of one instance of the Manager Service component must be installed. You can install one active instance and one backup instance of the Manager Service component to provide redundancy in a high-availability deployment.

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “Security Passphrase,” on page 29.
- (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 77.

Procedure

1 Disable any health checks for the load balancer and ensure that traffic is directed to the node.

2 Right-click the setup_vra-va-hostname.domain.name85480.exe setup file and select Run as administrator.

3 Accept the license agreement and click Next.
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.

9 Click **Next**.

10 Select **Manager Service** on the IaaS Server Custom Install page.

11 Type IaaS server information in the **IaaS Server** text box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, <code>IaaS-load-balancer.eng.mycompany.com</code>.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Type the fully qualified domain name of the IaaS Website Server. For example, <code>IaaS.eng.mycompany.com</code>.</td>
</tr>
</tbody>
</table>

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 Type the user name and password of the service account user who has administrative privileges on the current installation server in the Server Installation Information text boxes on the Server and Account Settings page.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have already installed components in this environment</td>
<td>Type the passphrase you created previously in the Passphrase and Confirm text boxes.</td>
</tr>
<tr>
<td>If this is the first installation</td>
<td>Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.</td>
</tr>
</tbody>
</table>

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 84.

A system administrator can change the authentication method used to access the SQL database during runtime (after the installation is complete). See “Configuring Windows Service to Access the IaaS Database,” on page 89.

Install a Backup Manager Service Component

You can install a passive backup instance of the Manager Service component that you can start manually to provide redundancy in a high-availability deployment.

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See “Security Passphrase,” on page 29.

- (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 77.

Procedure

1 Disable any health checks for the load balancer and ensure that traffic is directed to the node.
2 Right-click the setup__vra-va-hostname.domain.name@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.

10 Click Next.

11 Select Manager Service on the IaaS Server Custom Install page.

12 Type IaaS server information in the IaaS Server text box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Type the fully qualified domain name of the load balancer for the IaaS</td>
</tr>
<tr>
<td></td>
<td>Website Server. For example, IaaS-load-balancer.eng.mycompany.com.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Type the fully qualified domain name of the IaaS Website Server. For</td>
</tr>
<tr>
<td></td>
<td>example, IaaS.eng.mycompany.com.</td>
</tr>
</tbody>
</table>

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 Type the user name and password of the service account user who has administrative privileges on the current installation server in the Server Installation Information text boxes on the Server and Account Settings page.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have already installed components in this environment</td>
<td>Type the passphrase you created previously in the Passphrase and Confirm text boxes.</td>
</tr>
<tr>
<td>If this is the first installation</td>
<td>Type a passphrase in the Passphrase and Confirm text boxes. You must use this passphrase every time you install a new component.</td>
</tr>
</tbody>
</table>

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

If you will not add more nodes under the WEB load balancer, then enable applicable health checks.

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 runtime (after the installation is complete). See “Configuring Windows Service to Access the IaaS Database,” on page 89.

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**

A system administrator installs 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 IaaS Installer,” on page 71.

**Procedure**

1. Right-click the setup\_vra–va–hostname.domain.name@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.
9. Click **Next**.
10. Check prerequisites and click **Next**.
11. Enter the log in credentials under which the service will run. This must be a local administrator account.
12. Click **Next**.
13. Select the installation type from the **DEM role** drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worker</strong></td>
<td>The Worker executes workflows.</td>
</tr>
<tr>
<td><strong>Orchestrator</strong></td>
<td>The Orchestrator oversees DEM worker activities, including scheduling and preprocessing workflows, and monitors DEM worker online status.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If you are using a load balancer</strong></td>
<td>Type the fully qualified domain names of the load balancers for the Manager Service and Model Manager Web Service. For example, manager-load-balancer.eng.mycompany.com:443 and web-load-balancer.eng.mycompany.com:443.</td>
</tr>
<tr>
<td><strong>With no load balancer</strong></td>
<td>Type the fully qualified domain names of the Manager Service and Model Manager Web Service. For example, manager-service.eng.mycompany.com:443 and model-manager.eng.mycompany.com:443.</td>
</tr>
</tbody>
</table>

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\Logs.

Repeat this procedure to install additional DEM instances.

**Configure the DEM to Connect to SCVMM on a Nonstandard Installation Path**

By default, the DEM Worker configuration file (DynamicOps.DEM.exe.config) points to the standard installation path of Microsoft's System Center Virtual Machine Manager (SCVMM) console: {ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin. The system administrator must change the path if it is installed in another location.

This procedure is required only when you have SCVMM endpoints and agents.

**Prerequisites**

- If the SCVMM Console has been installed in another location, the configuration file of the DEM Worker (located in Program Files (x86)VMware\vCAC\Distributed Execution Manager\<InstanceName>\DynamicOps.DEM.exe.config) must be updated to change the default path in the assemblyLoadConfiguration section to point to the new folder.

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

1. Stop the DEM Worker.
2. Determine the installation path.
4. Restart the DEM Worker.

The default DEM Worker path is updated to the new folder.

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 72.
- 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 VMPS0psUser.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 VMPS0psUser.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 services account accesses the database during run-time, even if you created the database using SQL authentication. A system administrator can change the run-time authentication method from Windows, to SQL, when the database is on an untrusted domain, for example.

Prerequisites

“Choosing an IaaS Database Scenario,” on page 72.

Procedure

1. Log in to the Manager Service host as a local user with administrator privileges.
2. Stop the vCloud Automation Center service.
3. Navigate to the Server directory.
   `C:\Program Files (x86) \VMware\vCAC\Server\`
4. Open the `ManagerService.exe.config` file in a text editor.
5. In the `connectionStrings` section and the `serviceConfiguration serviceURI` section, replace `Integrated Security=True` with `User Id=DATABASE_USER;Password=DATABASE_PASSWORD`.
6. Save and close the file.
7. Navigate to `C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\`
8. Open the `Web.config` file in a text editor.
9. Locate the `repository server` section.
   `<repository server="localhost" database="vCAC" store="https://vcac.example.com/" />`
10. Add the database user command.
    `user=DATABASE_USER password=DATABASE_PASSWORD`. For example:
    `<repository server="localhost" database="vCAC" user="sqlUser" password="sqlPassword" store="https://vcac.example.com/" />`
11. Save and close the file.
12. Start the vCloud Automation Center Service.

SQL server authentication is now in use at run-time.

What to do next

Restart Internet Information Service.

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 Agent name
- VMware vCloud Automation Center Service

3 Close the Services window.

## Installing 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 93.

## 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.

### 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

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 4.16. Choosing an Agent Scenario

<table>
<thead>
<tr>
<th>Integration Scenario</th>
<th>Agent Requirements and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision cloud machines by integrating with a cloud environment such as Amazon Web Services or Red Hat Enterprise Linux OpenStack Platform.</td>
<td>You do not need to install an agent.</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a vSphere environment.</td>
<td>“Installing and Configuring the Proxy Agent for vSphere,” on page 92</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a Microsoft Hyper-V Server environment.</td>
<td>“Installing the Proxy Agent for Hyper-V or XenServer,” on page 97</td>
</tr>
</tbody>
</table>
| Provision virtual machines by integrating with a XenServer environment.              | ▪ “Installing the Proxy Agent for Hyper-V or XenServer,” on page 97  
▪ “Installing the EPI Agent for Citrix,” on page 104                                                                          |
| Provision virtual machines by integrating with a XenDesktop environment.             | ▪ “Installing the VDI Agent for XenDesktop,” on page 101  
▪ “Installing the EPI Agent for Citrix,” on page 104                                                                          |
| 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 106                                                            |
| 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 109                                                              |
| 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 `VRMAGen.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.

This table shows the detailed permissions the vSphere endpoint credentials must have to manage a vCenter Server instance.

<table>
<thead>
<tr>
<th>Attribute Value</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore</td>
<td>Allocate Space</td>
</tr>
<tr>
<td></td>
<td>Browse Datastore</td>
</tr>
<tr>
<td>Folder</td>
<td>Create Folder</td>
</tr>
<tr>
<td></td>
<td>Delete Folder</td>
</tr>
<tr>
<td>Global</td>
<td>Manage Custom Attributes</td>
</tr>
<tr>
<td></td>
<td>Set Custom Attribute</td>
</tr>
<tr>
<td>Network</td>
<td>Assign Network</td>
</tr>
<tr>
<td>Permissions</td>
<td>Modify Permission</td>
</tr>
<tr>
<td>Resource</td>
<td>Assign VM to Res Pool</td>
</tr>
<tr>
<td></td>
<td>Migrate Powered Off Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>Migrate Powered On Virtual Machine</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Inventory</td>
</tr>
<tr>
<td></td>
<td>Create from existing</td>
</tr>
<tr>
<td></td>
<td>Create New</td>
</tr>
<tr>
<td></td>
<td>Migrate Powered On Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>Move</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td>Interaction</td>
<td>Configure CD Media</td>
</tr>
<tr>
<td></td>
<td>Console Interaction</td>
</tr>
<tr>
<td></td>
<td>Device Connection</td>
</tr>
<tr>
<td></td>
<td>Power Off</td>
</tr>
<tr>
<td></td>
<td>Power On</td>
</tr>
<tr>
<td></td>
<td>Reset</td>
</tr>
<tr>
<td></td>
<td>Suspend</td>
</tr>
<tr>
<td></td>
<td>Tools Install</td>
</tr>
<tr>
<td>Configuration</td>
<td>Add Existing Disk</td>
</tr>
<tr>
<td></td>
<td>Add New Disk</td>
</tr>
<tr>
<td></td>
<td>Add or Remove</td>
</tr>
<tr>
<td></td>
<td>Remove Disk</td>
</tr>
</tbody>
</table>
Table 4-17. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

<table>
<thead>
<tr>
<th>Attribute Value</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td>Change CPU Count</td>
</tr>
<tr>
<td></td>
<td>Change Resource</td>
</tr>
<tr>
<td></td>
<td>Device Extend Virtual Disk Settings</td>
</tr>
<tr>
<td></td>
<td>Disk Change Tracking</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Modify Device Settings</td>
</tr>
<tr>
<td></td>
<td>Rename</td>
</tr>
<tr>
<td></td>
<td>Set Annotation (version 5.0 and later)</td>
</tr>
<tr>
<td></td>
<td>Settings</td>
</tr>
<tr>
<td></td>
<td>Swapfile Placement</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Customize</td>
</tr>
<tr>
<td></td>
<td>Clone Template</td>
</tr>
<tr>
<td></td>
<td>Clone Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>Deploy Template</td>
</tr>
<tr>
<td></td>
<td>Read Customization Specs</td>
</tr>
<tr>
<td>State</td>
<td>Create Snapshot</td>
</tr>
<tr>
<td></td>
<td>Remove Snapshot</td>
</tr>
<tr>
<td></td>
<td>Revert to Snapshot</td>
</tr>
</tbody>
</table>

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 93.
- If you already created a vSphere endpoint for use with this agent, make a note of the endpoint name.
- “Download the IaaS Installer,” on page 71.

Procedure

1. Right-click the setup_vra-va-hostname.domain.name@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.

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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent install</td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td>Single agent install</td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, manager-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, manager_service.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.
Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, <code>website-load-balancer.eng.mycompany.com:443</code>. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, <code>website_component.mycompany.com:443</code>. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

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

16 Enter the name of the endpoint.

   The endpoint name 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 96.

**Configure the vSphere Agent**

You can use the proxy agent utility to modify the initial configurations that are encrypted in the agent configuration file, or to change the machine deletion policy for virtualization platforms.

**Prerequisites**

Log in as a system administrator to the machine where you installed the agent.

**Procedure**

1 Open a Windows command console as an administrator.

2 Go to the agents installation directory.

   For example, `cd Program Files (x86)\VMware\vCAC\CD Agents\agent_name`.

3 (Optional) Enter `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` to view the current configuration settings.

   The following is an example of the output of the command:

   ```
   managementEndpointName: VCenterPoint
doDeletes: True
   ```
4  (Optional) Enter the `set managementEndpointName` command to change the name of the generic endpoint you configured at installation.

For example, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName My Endpoint`.

You change this property to rename the generic endpoint within vRealize Automation instead of changing endpoints.

5  (Optional) Enter the `set doDeletes` command to configure the virtual machine deletion policy.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>(Default) Delete virtual machines destroyed in vRealize Automation from vCenter Server.</td>
</tr>
<tr>
<td>false</td>
<td>Move virtual machines destroyed in vRealize Automation to the VRMDeleted directory in vCenter Server.</td>
</tr>
</tbody>
</table>

6  Navigate to **Start > Administrative Tools > Services** and restart the vRealize Automation Agent – `agentname` 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 IaaS Installer,” on page 71.

- 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_vra-va-hostname.domain.name@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.
7. Accept the root install location or click Change and select an installation 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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent install</td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td>Single agent install</td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>

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 Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, manager-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, manager_service.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

15 Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, website-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, website_component.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

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.
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 100.

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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The username representing administrator-level credentials for the XenServer or Hyper-V server the agent communicates with.</td>
</tr>
<tr>
<td>password</td>
<td>The password for the administrator-level username.</td>
</tr>
</tbody>
</table>

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 102 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 91.

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 101.
- “Download the IaaS Installer,” on page 71.

Procedure

1. Right-click the setup__vra-va-hostname.domain.name@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.
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.
Select VdiPowerShell from the Agent type list.

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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent install</td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td>Single agent install</td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>

Configure a connection to the Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, manager-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, manager_service.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, website-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, website_component.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

Click Test to verify connectivity to each host.

Select the VDI version.

Enter the fully qualified domain name of the managed server in the VDI Server text box.

Click Add.

Click Next.

Click Install to begin the installation.

After several minutes a success message appears.

Click Next.

Click Finish.

Verify that the installation is successful.

(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 104 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 91.

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 104.
- “Download the IaaS Installer,” on page 71.
Procedure

1. Right-click the setup_vra-va-hostname.domain.name@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.
7. Accept the root install location or click Change and select an installation 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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redundant agent install</strong></td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td><strong>Single agent install</strong></td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>
13 Configure a connection to the Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, manager-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, manager_service.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

14 Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, website-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, website_component.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>Credentials under which the agent will run must have administrative access to the installation host.</td>
</tr>
<tr>
<td>Microsoft PowerShell</td>
<td>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 <a href="http://support.microsoft.com">http://support.microsoft.com</a> for more information.</td>
</tr>
<tr>
<td>MS PowerShell Execution Policy</td>
<td>MS PowerShell Execution Policy must be set to <strong>RemoteSigned</strong> or <strong>Unrestricted</strong>. For information on PowerShell Execution Policy issue one of the following commands at Power-Shell command prompt: help about_signing help Set-ExecutionPolicy</td>
</tr>
</tbody>
</table>

### 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 107.
- “Download the IaaS Installer,” on page 71.

**Procedure**

1. Right-click the `setup__.vra-va-hostname.domain.name@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.

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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent install</td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td>Single agent install</td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, <strong>manager-load-balancer.eng.mycompany.com:443</strong>. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, <strong>manager_service.mycompany.com:443</strong>. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.
Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, website-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, website_component.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

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 109.
- “Download the IaaS Installer,” on page 71.

Procedure

1. Right-click the setup_vra-vamsgame_setupname@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.
7. Accept the root install location or click Change and select an installation 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** Do not duplicate agent names unless you are installing redundant, identically configured agents for high availability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent install</td>
<td>Install redundant agents on different servers, but name and configure them identically to provide high-availability.</td>
</tr>
<tr>
<td>Single agent install</td>
<td>Select a unique name for this agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the Manager Service component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component. For example, manager-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component. For example, manager_service.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

The default port is 443.

14 Configure a connection to the Manager Website component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Website component. For example, website-load-balancer.eng.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
<tr>
<td>With no load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Website component. For example, website_component.mycompany.com:443. IP addresses are not recognized.</td>
</tr>
</tbody>
</table>

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.
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 the vRealize Automation console as the system administrator of the default tenant.
   a. Navigate to the vRealize Automation console.
   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.
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.
Troubleshooting

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 117
- “Rolling Back a Failed Installation,” on page 118
- “Create a Support Bundle for vRealize Automation,” on page 120
- “General Installation Troubleshooting,” on page 120
- “Troubleshooting vRealize Automation Appliances,” on page 123
- “Troubleshooting IaaS Components,” on page 125
- “Troubleshooting Log-In Errors,” on page 131

Default Log Locations

Consult system and product log files for information on a failed installation.

The file paths shown are the default paths. If you installed IaaS in another directory, navigate to your custom installation directory instead.

**Note** The VMware vRealize™ Automation (vRA) content pack for vRealize Log Insight provides a consolidated summary of log events in all of the vRealize Automation components. For more information, see the vRA 6.1+ Log Insight Content Pack description on VMware Solution Exchange at https://solutionexchange.vmware.com/store/products/vra-6-1-log-insight-content-pack#.VU0r3_PD-Ht.

Windows Logs

Use the following to find log files for Windows events.

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Event Viewer logs</td>
<td><strong>Start &gt; Control Panel &gt; Administrative Tools &gt; Event Viewer</strong></td>
</tr>
</tbody>
</table>

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\Logs
Repository Log | C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Manager Service Logs | C:\Program Files (x86)\VMware\vCAC\Server\Logs
DEM Orchestrator Logs | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs
Agent Logs | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs
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.

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.

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 7-1. Roll Back Failure Points

<table>
<thead>
<tr>
<th>Failure Point</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing Manager Service</td>
<td>If present, uninstall vCloud Automation Center Server.</td>
</tr>
<tr>
<td>Installing DEM-Orchestrator</td>
<td>If present, uninstall the DEM Orchestrator.</td>
</tr>
<tr>
<td>Installing DEM-Worker</td>
<td>If present, uninstall all DEM Workers</td>
</tr>
<tr>
<td>Installing an Agent</td>
<td>If present, uninstall all vRealize Automation agents.</td>
</tr>
</tbody>
</table>

Create a Support Bundle for vRealize Automation

A root user can create a support bundle in the vRealize Automation appliance management console or for IaaS components. These bundles can help VMware support staff to identify causes of issues you might encounter.

For information about creating a support bundle for IaaS component see the VMware Knowledge Base article Collecting VMware vRealize Automation logs using the log collection utility (2078179) at http://kb.vmware.com/kb/2078179.

Use the following procedure to create a support bundle for vRealize Automation appliance.

Procedure


2. Log in and go to Admin > Logs.

3. Click Create support bundle.

4. Click Download and save the file on your system.

You can use the support bundle to troubleshoot issues on your own or to send to your VMware support representative.

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.
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 49
- “Enable Time Synchronization on the Windows Server,” on page 52

For an overview of timekeeping for vRealize Automation, see “Time Synchronization,” on page 29.

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 the vcac-config.exe.config file and locate the repository address:
   ```xml
   <add key="repositoryAddress" value="https://[IaaS address]:443/repository/" />
   ```
2. Browse to the address with Internet Explorer.
3. Continue through any error messages about certificate trust issues.
4. Obtain a security report from Internet Explorer and use it to troubleshoot why this 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. Point a Web browser to the vRealize Automation appliance management console:
   ```text
   https://appliance-FQDN-or-IP-address:5480
   ```
2. Log in with the user name root and the password that you set when you deployed the appliance.
3. Click the Network tab.
4. Enter your site proxy server FQDN or IP address, and port number.
5. If your proxy server requires credentials, enter the user name and password.
6. 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 123.

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 122.

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=
vra-hostname
   For example:
   NO_PROXY="localhost, 127.0.0.1, vra.system.mycompany.com"
4. Save and close proxy.
5. Restart the Horizon workspace service by entering the following command.
   service horizon-workspace restart

Troubleshooting vRealize Automation Appliances

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__vra-va-hostname.domain.name.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 appliance by typing the following URL in a Web browser.
   
   https://vra-va-hostname.domain.name

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` 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. Run the following SQL query:
   ```sql
   UPDATE "databasechangeloglock" SET locked=FALSE, lockgranted=NULL, lockedby=NULL WHERE id=1;
   ```
6. Run the SQL query `select * from databasechangeloglock`
   The output should show a value of "f" for locked.
7. Start the horizon-workspace service using the command `service horizon-workspace start`.

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:
   
   Certificate 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 msiexec 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
  Check that you can connect to the vRealize Automation appliance by typing the following URL in a Web browser: https://vra-va-hostname.domain.name.
- Trusted Certificate Issues
  - In IaaS, open Microsoft Management Console with the command \%mc.exe and check that the certificate used in the installation has been added to the Trusted Root Certificate Store in the machine.
  - From a browser check https://<ip-web>/repository/data/MetaModel.svc and verify that no certificate errors appear in your browser.
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 browser, check the status of the MetaModel service at `https://<ip-web>/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.

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 the Microsoft Knowledge Base article at http://support.microsoft.com/kb/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 appliance.
      https://virtualappliancename(vcacc/tenantname
   b Navigate to Infrastructure > Managed Machines.
   c Right click on 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
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 @<em>yourdomain</em> portion of the user name, you are logged out of SSO immediately and redirected to the login page with no explanation. </li>

Cause

The UPN entered must adhere to a <em>yourname.admin@yourdomain</em> 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 @<em>yourdomain</em> 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.

Cannot Log in to a Tenant or Tenant Identity Stores Disappear

Ninety days after deployment, you cannot log into a tenant or the identity store for a tenant disappears.

Problem

- When you log in to a tenant, you see a blank page displayed with a Submit button in the upper left-hand corner.
- You receive a System Exception error when accessing the tenant ID store configuration page.
- The ID store configuration disappears.
- You cannot log in to a tenant by using an LDAP account.
- The catalina.out log located in /var/log/vmware/vcac/ shows an error similar to the following:
12:40:49,190 [tomcat-http--34] [authentication] INFO
com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl
$RequestResponseProcessor.handleFaultCondition:922 - Failed trying to retrieve token:
ns0:RequestFailed: Error occurred looking for solution user :: Insufficient access YYYY-03-18
12:40:49,201 [tomcat-http--34] [authentication] ERROR
com.vmware.vcac.platform.service.rest.resolver.ApplicationExceptionHandler.handleUnexpectedException:820 - Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for solution user :: Insufficient access com.vmware.vim.sso.client.exception.InternalError: Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for solution user :: Insufficient access

Cause
The SSO internal tenant administrator password expires after 90 days by default. This issue is internal to vRealize Automation and does not affect external, Active Directory identity stores.

It is a known issue that the vRealize Automation user interface does not provide notification that the tenant administrator password is expiring. The workaround for this issue is to disable password expiration for the tenant administrator account.

For step-by-step instructions to resolve this issue, see the VMware knowledge base article at http://kb.vmware.com/kb/2075011.
Index

A
account settings, specifying 55
agents
  choosing the installation scenario 92
configuring Hyper-V 100
configuring XenServer 100
configuring vSphere agents 96
  enabling remote WMI requests 109
EPI Powershell 16
Hyper-V 97
  installation location and requirements 92
  installing 91
  installing WMI 110
  installing XenDesktop 102
  installing Citrix agents 104
  installing EPI agent for Citrix 104
  installing for Visual Basic scripting 107
  installing the EPI agent for VB scripting 106
  installing vSphere agents 94
  integration agents 16
VDI PowerShell 16
Visual Basic scripting requirements 107
WMI agents 16
XenServer 97
  appliances, configuring additional 67

C
certificate chains, order 28
certificate validation 125
certificate name mismatch 127
certificates
  switching from self-signed 115
trust relationships 59
chained certificates, order 28
Citrix, installing the EPI agent 104
Citrix agents, installing 104
Cloned IaaS nodes 130
clusters, joining 68
  configure, vRealize Automation appliance 64
database
  creating by using the wizard 75
  preparing IaaS database 72
requirements 21
DEM
  about installing 86
  installing 87
requirements 23
DEM Worker, connecting to SCVMM 88
dems
  Amazon Web Services EC2 requirements 23
  Red Hat requirements 23
  SCVMM requirements 24
DEM, install fails 126
deployment parameters, specifying 37, 44
deployment scenario
  distributed deployment 57
  minimal deployment 47
  minimal installation 11
deployment path
  choosing 11
distributed installation 11
distributed deployment
  disable unused services 69
  install with wizard 40
  installation overview 13
  validating 69
Distributed Execution Managers, See also DEM
distributed installation
  overview 57
  uninstalling 119
Distributed Transaction Coordinator (DTC) 21
Distributed Execution Manager, See DEM
DTC (Distributed Transaction Coordinator) 21
E
Email customizations 130
Encryption.key file, setting permissions 124
Enterprise deployment, install with wizard 40
EPI agents, installing for Visual Basic scripting 106, 107
F
failed installation, logs 117
H
Hyper-V
  agent 97
proxy agent 97
requirements 97
Hyper-V agents, installing 97
hypervisor, requirements 97

IaaS
agents 16
download installer 71
IaaS administrators, creating 113
IaaS components
installing 52
installing in a distributed configuration 69
registering 56
troubleshooting 125
IaaS components, definitions 58
IaaS installer
downloading 54
troubleshooting 126
IaaS services, verifying 90
IaaS Authentication, failure 127
IaaS administrator login fails 131
IaaS database
configuring for secure SSL 55, 72–75
configuring Windows service for access 89
configuring Windows services account to use SQL authentication 90
creating the database 74
creating the database manually 73
creating the database using the wizard 75
specifying the SQL database 55
IaaS database access, enabling from service user 89
IaaS distributed installation 58
IaaS Manager Service, requirements 22
Identity stores, troubleshooting 131
identity manager, fails to start 124
identity store, domain requirements 26
infrastructure components, installing 53
Initial content configuration, create password 39, 46
installation
completing 57
configuring 117
distributed deployment overview 13
DNS and host name resolution 19
finishing 38, 45
minimal deployment overview 12
minimal installation overview 47
overview 11
preparation 19
specifying agents 56
specifying managers 56
troubleshooting 117
vRealize Automation appliance 48, 63
Installation, using the management console 47
installation components
checking prerequisites 55
choosing a deployment path 11
SSO 14
VMware Infrastructure as a Service (IaaS) 15
VMware vRealize Automation appliance 15
installation parameter, validation 38, 45
installation preparation, time synchronization 29
installation requirements
credentials 26
deployment environments 19
hardware 19
IaaS requirements 21
operating system 19
port requirements 24
security 28
users 26
virtual machine 19
Windows server 21
XenDesktop 101
Installation troubleshooting 120
installation wizard, enterprise deployment 40
Installation Wizard, overview 31
installation download, troubleshooting 123
installation failure, servers out of sync 121
installation type
logging in 54
selecting 54
installing
browser considerations 20
configuring vCloud Automation Center Appliances 63
download IaaS installer 71
worksheet 60
internal error, adding XaaS endpoint 128

J
Java requirements, for MSSQL database 21

L
load balancers, configuring 63
load balancer times out before completion,
changing the load balancer timeout setting 120
Log in errors, troubleshooting 131
login failure, servers out of sync 121
logs, locations 117
Logs
IaaS 117
troubleshooting 117
machine request fails 129
Management Agent
  install 34, 41
  installing 34, 40
  uninstall 34, 41
Management Agent SSL fingerprint, locating 34, 41
Manager service, definition 58
Manager Service
  installing 82, 84
  requirements 22
minimal deployment, installation overview 12
minimal installation, uninstalling 118
Minimal deployments, install with installation wizard 33
Model Manager
  definition 58
  editable business logic 15
  execution policies 15
  secure multi-tenancy 15
  troubleshooting install failures 127
  unified data model 15
Model Manager data, installing 77, 78, 80
  Model Manager Web 15
password, restrictions 20
PEM files, command for extracting 28
post-installation tasks, configuring Windows service to access IaaS database 89
PowerShell, setting to RemoteSigned 91
Prerequisite Checker, run in Installation Wizard 36, 43
prerequisites
  browser considerations 20
  checking 55
  provisioning server 104
proxy 123
proxy agent, uninstall fails 129
proxy agents, installing and configuring for vSphere 92
requirements
database 21
DEM 23
SQL 21
RSA private keys, command for extracting 28
scenarios, choosing the agent installation 92
security certificates 28
IaaS certificates 53, 71
passphrase 29
third-party software 29
trust relationships 59
server settings, specifying 55
server requirements, IaaS or Windows server 21
snapshots, creating 37, 44
SQL, requirements 21
SSL certificates, extracting 28
support bundle, creating 120
System error message 124
tenants
  configuring default tenant 113
  troubleshooting ID stores 131
  troubleshooting login 131
time synchronize, servers 49, 67
time sync, enabling on Windows machine 52
troubleshooting
  blank pages appearing 121
  cloned IaaS nodes 130
  IaaS installer 126
  log locations 117
  machine requests 129
  server times out of sync 121
  trusted certificate issues 127
uninstall, failed installation 118, 119
Uninstall, failed installation 118
updated information 9
vCloud Suite, licensing 7
VDI agent for XenDesktop, installing 101
virtual appliance time settings, with the Installation Wizard 36, 43
virtualization proxy agents 16
Visual Basic, scripting requirements 107
Visual Basic scripting
  installing EPI agents 107
  installing the EPI agent 106
VMware Identity Manager 123
VMware IaaS
  distributed execution manager 16
  manager service 15
  VMware IaaS, database 15
  VMware IaaS, IaaS Website 15
  VMware IaaS, Model Manager 15
vRealize Appliance
  configuring 50
  deploying 31, 48
vRealize Automation appliances,
  troubleshooting 123
vRealize Realize Automation appliance 48
vRealize Appliance clusters; joining 68
vRealize Automation appliance, deploying 61
vRealize Orchestrator, use external for high-availability deployments 57
vSphere agents
configuring 96
installing 94
vSphere agent
required permissions 93
supported configuration for concurrency 93
vSphere proxy agents, installing and configuring 92

W
WAPI, install fails 126
website component, installing 77, 78, 80
Windows services account, configuring to use SQL authentication 90
WMI agents
enabling remote requests 109
installing 110

X
XenDesktop
installation requirements 101
installing agent 102
installing VDI agent 101
XenServer
agent 97
proxy agent 97
XenServer agents, installing 97
XenServer Host name, setting 102