Installing vRealize Automation

05 October 2018

vRealize Automation 7.4

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Updated Information

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

Revision	Description
5 OCT 2018	■ Removed IIS requirement in IaaS Manager Service Host. ■ Added reference to increased hardware in IaaS SQL Server Host. ■ Added certificate FQDN prerequisite to Install Additional IaaS Web Server Components and Install a Backup Manager Service Component. ■ Added 25 agent limit in the online Help.
15 JUN 2018	Added .NET 3.5 to prerequisites in IaaS Windows Servers.
3 MAY 2018	■ Added vRealize Suite Lifecycle Manager to About vRealize Automation Installation. ■ Added Windows 2016 to IaaS Web Server and IaaS Manager Service Host. ■ Expanded the Java requirement to Java 1.8 update 161 or later. ■ Restored certificate prerequisite in Configure the vRealize Automation Appliance. ■ Removed outdated 6.2 reference in Install the Distributed Execution Managers.
12 APR 2018	Initial document release.

vRealize Automation Installation

This *vRealize Automation Installation* guide contains wizard, manual, and silent installation instructions for VMware vRealize ™ Automation.

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

Intended Audience

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

VMware Technical Publications Glossary

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

vRealize Automation Installation Overview

1

You can install vRealize Automation to support minimal, proof of concept environments, or in different sizes of distributed, enterprise configurations that are capable of handling production workloads. Installation can be interactive or silent.

After installation, you start using vRealize Automation by customizing your setup and configuring tenants, which provides users with access to self-service provisioning and life-cycle management of cloud services.

This chapter includes the following topics:

About vRealize Automation Installation

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

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

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

You can also install vRealize Automation using vRealize Suite Lifecycle Manager. See the vRealize Suite documentation.

New in this vRealize Automation Installation

If you installed earlier versions of vRealize Automation, be aware of changes in the installation for this release before you begin.

- This release simplifies the vRealize Automation appliance renaming process. See Change the vRealize Automation Appliance Host Name.
- In this release, the vRealize Automation appliance uses TLS 1.2 by default. The administration interface includes an option to temporarily enable TLS 1.0 and 1.1, which is needed for updating existing agents to this release.
- The vRealize Automation appliance administration interface now includes a page for installing and managing patches. See Access Patch Management.
- This release describes how to change the default proxy port for VMware Remote Console. See Change the VMware Remote Console Proxy Port.
- This release fixes some broken Help links in the installation wizard.

vRealize Automation Installation Components

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

The vRealize Automation Appliance

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

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

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

  In large deployments with redundant appliances, the secondary appliance databases serve as replicas to provide high availability.
- The appliance includes a preconfigured instance of vRealize Orchestrator. vRealize Automation uses vRealize Orchestrator workflows and actions to extend its capabilities.

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

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

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

Infrastructure as a Service

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

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

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

Web Server

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

Model Manager

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

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

Manager Service

The Manager Service is a Windows service that coordinates communication between IaaS DEMs, the SQL Server database, agents, and SMTP. In addition, the Manager Service communicates with the Web server through the Model Manager and must be run under a domain account with local administrator privileges on all IaaS Windows servers.

Unless you enable automatic Manager Service failover, IaaS requires that only one Windows machine actively runs the Manager Service at a time. For backup or high availability, you may deploy additional Manager Service machines, but the manual failover approach requires that backup machines have the service stopped and configured to start manually.

For more information, see About Automatic Manager Service Failover.

SQL Server Database

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

Distributed Execution Manager

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

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

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

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

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

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

Agents

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

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

Virtualization Proxy Agents

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

A virtualization proxy agent has the following characteristics.

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

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

Virtual Desktop Integration Agents

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

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

External Provisioning Integration Agents

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

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

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

Windows Management Instrumentation Agent

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

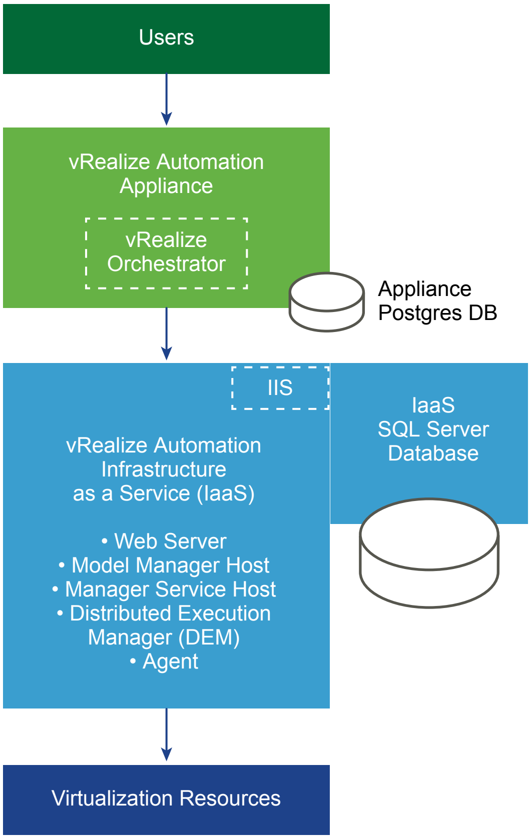
Deployment Type

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

Minimal vRealize Automation Deployments

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

Figure 1-1. Minimal vRealize Automation Deployment



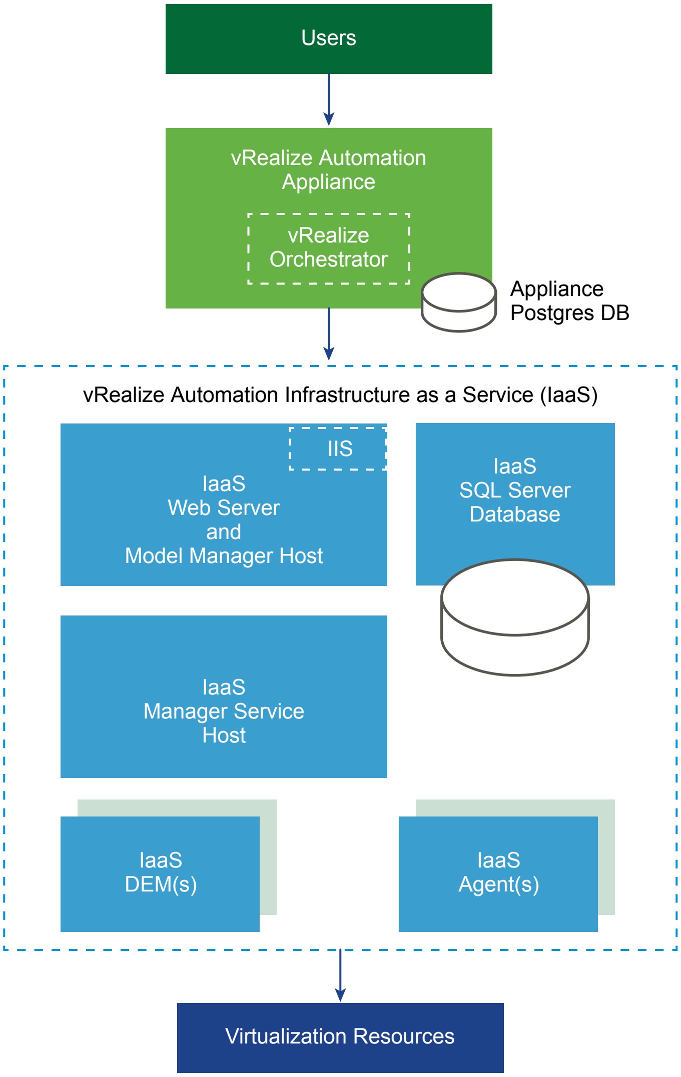
You cannot convert a minimal deployment to an enterprise deployment. To scale a deployment up, start with a small enterprise deployment, and add components to that. Starting with a minimal deployment is not supported.

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

Distributed vRealize Automation Deployments

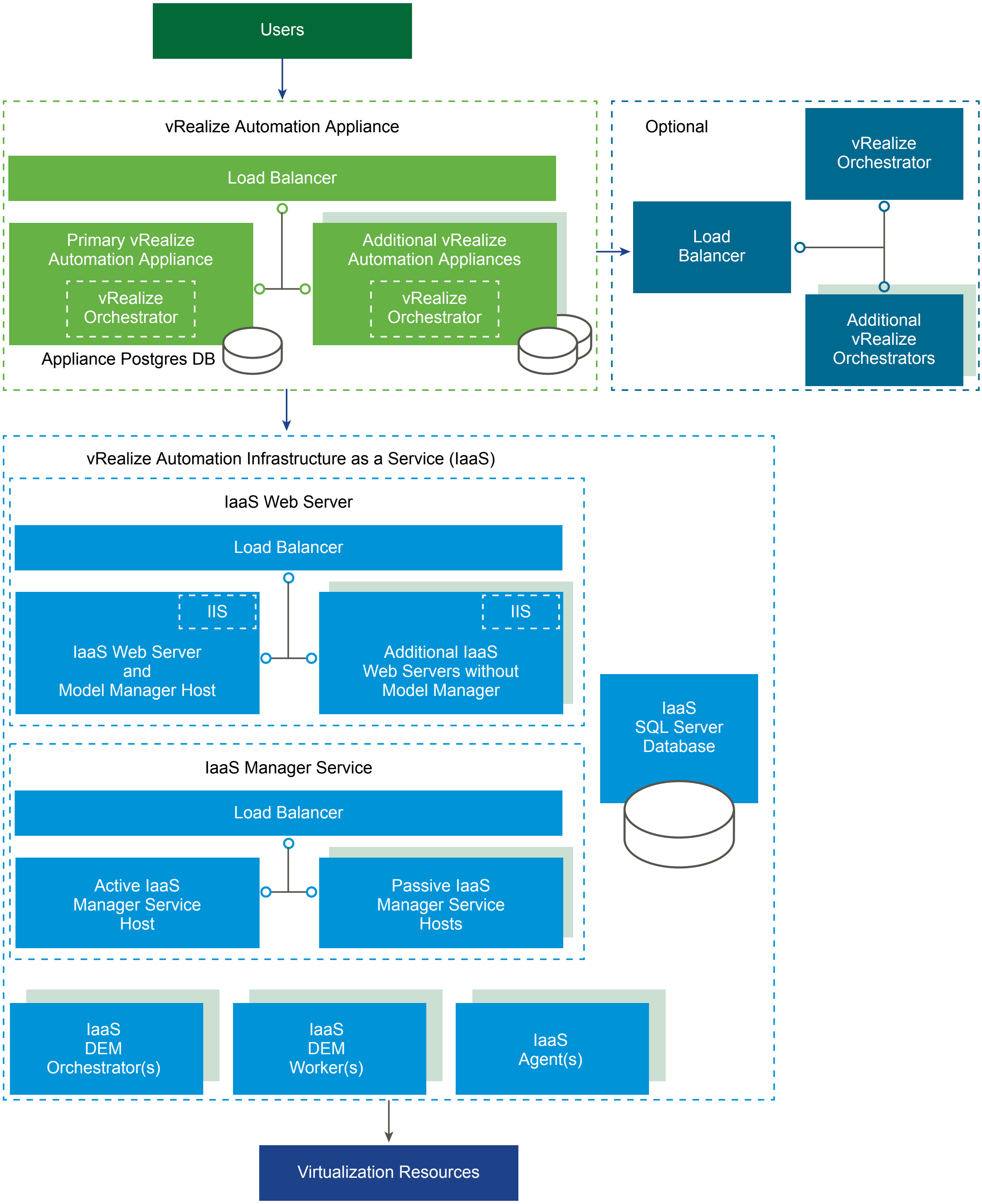
Distributed, enterprise deployments can be of varying size. A basic distributed deployment might improve vRealize Automation simply by hosting IaaS components on separate Windows servers as shown in the following figure.

Figure 1-2. Distributed vRealize Automation Deployment


Users
vRealize Automation Appliance
vRealize Orchestrator
Appliance Postgres DB
vRealize Automation Infrastructure as a Service (IaaS)
IIS
IaaS Web Server and Model Manager Host
IaaS SQL Server Database
IaaS Manager Service Host
IaaS DEM(s)
IaaS Agent(s)
Virtualization Resources

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

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


Users
vRealize Automation Appliance
Load Balancer
Primary vRealize Automation Appliance
vRealize Orchestrator
Appliance Postgres DB
Additional vRealize Automation Appliances
vRealize Orchestrator
Optional
vRealize Orchestrator
Load Balancer
Additional vRealize Orchestrators
vRealize Automation Infrastructure as a Service (IaaS)
IaaS Web Server
Load Balancer
IIS
IaaS Web Server and Model Manager Host
IIS
Additional IaaS Web Servers without Model Manager
IaaS SQL Server Database
IaaS Manager Service
Load Balancer
Active IaaS Manager Service Host
Passive IaaS Manager Service Hosts
IaaS DEM Orchestrator(s)
IaaS DEM Worker(s)
IaaS Agent(s)
Virtualization Resources

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

Choosing Your Installation Method

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

- The Installation Wizard provides a simple and fast way to install, from minimal deployments to distributed enterprise deployments with or without load balancers. Most users run the Installation Wizard.
- If you want to expand a vRealize Automation deployment or if the Installation Wizard stopped for any reason, you need the manual installation steps. After you begin a manual installation, you cannot go back and run the Installation Wizard.
- Depending on your site needs, you might also take advantage of silent, command line or API-based installation.

Preparing for vRealize Automation Installation

2

You install vRealize Automation into existing virtualization infrastructure. Before you begin an installation, you need to address certain environmental and system requirements.

This chapter includes the following topics:

General Preparation

There are several deployment-wide considerations to be aware of before installing vRealize Automation.

For more about high-level environment requirements, including supported operating system and browser versions, see the vRealize Automation Support Matrix.

User Web Browsers

Multiple browser windows and tabs are not supported. vRealize Automation supports one session per user.

VMware Remote Consoles provisioned on vSphere support only a subset of vRealize Automation supported browsers.

Third Party Software

All third-party software should have the latest vendor patches. Third party software includes Microsoft Windows and SQL Server.

Time Synchronization

All vRealize Automation appliances and IaaS Windows servers must synchronize to the same time source. You may use only one of the following sources. Do not mix time sources.

- The vRealize Automation appliance host
- One external network time protocol (NTP) server

To use the vRealize Automation appliance host, you must run NTP on the ESXi host. For more about timekeeping, see VMware Knowledge Base article 1318.

You select the time source on the Installation Prerequisites page of the Installation Wizard.

Accounts and Passwords

There are several user accounts and passwords that you might need to create or plan settings for, before installing vRealize Automation.

IaaS Service Account

IaaS installs several Windows services that must run under a single user account.

- The account must be a domain user.
- The account does not need to be a domain administrator, but must have local administrator permission, before installation, on all IaaS Windows servers.
- The account password cannot contain a double quotation mark (") character.
- The Management Agent installer for IaaS Windows servers prompts you for the account credentials.
- The account must have **Log on as a service** permission, which lets the Manager Service start and generate log files.
- The account must have dbo permission on the IaaS database.

  If you use the installer to create the database, add the account login to SQL Server before installation. The installer grants the dbo permission after it creates the database.
- If you use the installer to create the database, in SQL, add the sysadmin role to the account before installation.

  The sysadmin role is not required if you choose to use a pre-existing empty database.

IIS Application Pool Identity

The account you use as the IIS application pool identity for the Model Manager Web service must have **Log on as batch job** permission.

IaaS Database Credentials

You can let the vRealize Automation installer create the database, or you can create it separately using SQL Server. When the vRealize Automation installer creates the database, the following requirements apply.

- For the vRealize Automation installer, if you select Windows Authentication, the account that runs the Management Agent on the primary IaaS Web server must have the sysadmin role in SQL to create and alter the size of the database.
- For the vRealize Automation installer, even if you do not select Windows Authentication, the account that runs the Management Agent on the primary IaaS Web server must have the sysadmin role in SQL because the credentials are used at runtime.
- If you separately create the database, the Windows user or SQL user credentials that you provide only need dbo permission on the database.

IaaS Database Security Passphrase

The database security passphrase generates an encryption key that protects data in the IaaS SQL database. You specify the security passphrase on the IaaS Host page of the Installation Wizard.

- Plan to use the same database security passphrase across the entire installation so that each component has the same encryption key.
- Record the passphrase, because you need the passphrase to restore the database if there is a failure or to add components after initial installation.
- The database security passphrase cannot contain a double quotation mark (") character. The passphrase is accepted when you create it but causes the installation to fail.

vSphere Endpoints

If you plan to provision to a vSphere endpoint, you need a domain or local account with enough permission to perform operations on the target. The account also needs the appropriate level of permission configured in vRealize Orchestrator.

vRealize Automation Administrator Password

After installation, the vRealize Automation administrator password logs you in to the default tenant. You specify the administrator password on the Single Sign-On page of the Installation Wizard.

The vRealize Automation administrator password cannot contain a trailing equals (=) character. The password is accepted when you create it but results in errors later, when you perform operations such as saving endpoints.

Host Names and IP Addresses

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

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

  While performing the installation, always enter the complete FQDN when identifying or selecting a vRealize Automation machine. Do not enter IP addresses or short machine names.

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

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

- Preplan domain and machine naming so that vRealize Automation machine names begin with letters (a–z, A–Z), end with letters or digits (0–9), and have only letters, digits, or hyphens (-) in the middle. The underscore character (_) must not appear in the host name or anywhere in the FQDN.

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

- In general, you should expect to keep the host names and FQDNs that you planned for vRealize Automation systems. Changing a host name is not always possible. When a change is possible, it might be a complicated procedure.

- A best practice is to reserve and use static IP addresses for all vRealize Automation appliances and IaaS Windows servers. vRealize Automation supports DHCP, but static IP addresses are recommended for long-term deployments such as production environments.

  - You apply an IP address to the vRealize Automation appliance during OVF or OVA deployment.
  - For the IaaS Windows servers, you follow the usual operating system process. Set the IP address before installing vRealize Automation IaaS.

Latency and Bandwidth

vRealize Automation supports multiple site, distributed installation, but data transmission speed and volume must meet minimum prerequisites.

vRealize Automation needs an environment of 5 ms or lower network latency, and 1 GB or higher bandwidth, among the following components.

- vRealize Automation appliance
- IaaS Web server

- IaaS Model Manager host
- IaaS Manager Service host
- IaaS SQL Server database
- IaaS DEM Orchestrator

The following component might work at a higher latency site, but the practice is not recommended.

- IaaS DEM Worker

You may install the following component at the site of the endpoint with which it communicates.

- IaaS Proxy Agent

vRealize Automation Appliance

Most vRealize Automation appliance requirements are preconfigured in the OVF or OVA that you deploy. The same requirements apply to standalone, master, or replica vRealize Automation appliances.

The minimum virtual machine hardware on which you can deploy is Version 7, or ESX/ESXi 4.x or later. See VMware Knowledge Base article 2007240. Because of the hardware resource demand, do not deploy on VMware Workstation.

After deployment, you might use vSphere to adjust vRealize Automation appliance hardware settings to meet Active Directory requirements. See the following table.

Table 2‑1. vRealize Automation Appliance Hardware Requirements for Active Directory

vRealize Automation Appliance for Small Active Directories	vRealize Automation Appliance for Large Active Directories
■ 4 CPUs ■ 18 GB memory ■ 60 GB disk storage	■ 4 CPUs ■ 22 GB memory ■ 60 GB disk storage

A small Active Directory has up to 25,000 users in the organizational unit (OU) to be synced in the ID Store configuration. A large Active Directory has more than 25,000 users in the OU.

vRealize Automation Appliance Ports

Ports on the vRealize Automation appliance are usually preconfigured in the OVF or OVA that you deploy.

The following ports are used by the vRealize Automation appliance.

Table 2‑2. Incoming Ports

Port	Protocol	Comments
22	TCP	Optional. Access for SSH sessions.
80	TCP	Optional. Redirects to 443.
88	TCP (UDP optional)	Cloud KDC Kerberos authentication from external mobile devices.
443	TCP	Access to the vRealize Automation console and API calls.

Table 2‑2. Incoming Ports (Continued)

Port	Protocol	Comments
		Access for machines to download the guest agent and software bootstrap agent.
		Access for load balancer, browser.
4369, 5671, 5672, 25672	TCP	RabbitMQ messaging.
5480	TCP	Access to the virtual appliance management interface.
		Used by the Management Agent.
5488, 5489	TCP	Internally used by the vRealize Automation appliance for updates.
8230, 8280, 8281, 8283	TCP	Internal vRealize Orchestrator instance.
8443	TCP	Access for browser. Identity Manager administrator port over HTTPS.
8444	TCP	Console proxy communication for vSphere VMware Remote Console connections.
9300–9400	TCP	Access for Identity Manager audits.
54328	UDP	

Table 2‑3. Outgoing Ports

Port	Protocol	Comments
25, 587	TCP, UDP	SMTP for sending outbound notification email.
53	TCP, UDP	DNS server.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Optional. For fetching software updates. Updates can be downloaded separately and applied.
88, 464, 135	TCP, UDP	Domain controller.
110, 995	TCP, UDP	POP for receiving inbound notification email.
143, 993	TCP, UDP	IMAP for receiving inbound notification email.
123	TCP, UDP	Optional. For connecting directly to NTP instead of using host time.
389	TCP	Access to View Connection Server.
389, 636, 3268, 3269	TCP	Active Directory. Default ports shown, but are configurable.
443	TCP	Communication with IaaS Manager Service and infrastructure endpoint hosts over HTTPS.
		Communication with the vRealize Automation software service over HTTPS.
		Access to the Identity Manager upgrade server.
		Access to View Connection Server.
445	TCP	Access to ThinApp repository for Identity Manager.
902	TCP	ESXi network file copy operations and VMware Remote Console connections.
5050	TCP	Optional. For communicating with vRealize Business for Cloud.

Table 2-3. Outgoing Ports (Continued)

Port	Protocol	Comments
5432	TCP, UDP	Optional. For communicating with another appliance PostgreSQL database.
5500	TCP	RSA SecurID system. Default port shown, but is configurable.
8281	TCP	Optional. For communicating with an external vRealize Orchestrator instance.
9300–9400	TCP	Access for Identity Manager audits.
54328	UDP	

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.

IaaS Windows Servers

All Windows servers that host IaaS components must meet certain requirements. Address requirements before you run the vRealize Automation Installation Wizard or the standard Windows-based installer.

- Place all IaaS Windows servers on the same domain. Do not use Workgroups.
- Each server needs the following minimum hardware.
  - 2 CPUs
  - 8 GB memory
  - 40 GB disk storage

  A server that hosts the SQL database together with IaaS components might need additional hardware.
- Because of the hardware resource demand, do not deploy on VMware Workstation.
- Install Microsoft .NET Framework 3.5.
- Install Microsoft .NET Framework 4.5.2 or later.

  A copy of .NET is available from any vRealize Automation appliance:

  https://*vrealize-automation-appliance-fqdn*:5480/installer/

  If you use Internet Explorer for the download, verify that Enhanced Security Configuration is disabled. Navigate to res://iesetup.dll/SoftAdmin.htm on the Windows server.
- Install Microsoft PowerShell 2.0, 3.0, or 4.0, based on your version of Windows.

  Note that some vRealize Automation upgrades or migrations might require an older or newer PowerShell version, in addition to the one that you are currently running.
- If you install more than one IaaS component on the same Windows server, plan to install them to the same installation folder. Do not use different paths.
- IaaS servers use TLS for authentication, which is enabled by default on some Windows servers.

  Some sites disable TLS for security reasons, but you must leave at least one TLS protocol enabled. This version of vRealize Automation supports TLS 1.2.

- Enable the Distributed Transaction Coordinator (DTC) service. 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.

  Also enable DTC on the server that hosts the SQL database, if it is separate from IaaS. For more about DTC enablement, see VMware Knowledge Base article 2038943.

- Verify that the Secondary Log On service is running. If desired, you may stop the service after installation is complete.

IaaS Windows Server Ports

Ports on the IaaS Windows servers must be configured before vRealize Automation installation.

Open ports between all IaaS Windows servers according to the following tables. Include the server that hosts the SQL database, if it is separate from IaaS. Alternatively, if site policies allow, you may disable firewalls between IaaS Windows servers and SQL Server.

Table 2-4. Incoming Ports

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

Table 2-5. Outgoing Ports

Port	Protocol	Component	Comments
53	TCP, UDP	All	DNS
67, 68, 546, 547	TCP, UDP	All	DHCP
123	TCP, UDP	All	Optional. NTP
443	TCP	Manager Service	Communication with vRealize Automation appliance over HTTPS

Table 2-5. Outgoing Ports (Continued)

Port	Protocol	Component	Comments
443	TCP	Distributed Execution Managers	Communication with Manager Service over HTTPS
443	TCP	Proxy agents	Communication with Manager Service and infrastructure endpoint hosts over HTTPS
443	TCP	Management Agent	Communication with the vRealize Automation appliance
443	TCP	Guest agent Software bootstrap agent	Communication with Manager Service over HTTPS
1433	TCP	Manager Service Website	MSSQL
5480	TCP	All	Communication with the vRealize Automation appliance.

Also, because you enable DTC between all servers, DTC requires port 135 over TCP and a random port between 1024 and 65535. Note that the Prerequisite Checker validates that DTC is running and the required ports are open.

IaaS Web Server

A Windows server that hosts the Web component must meet additional requirements, in addition to those for all IaaS Windows servers.

The requirements are the same, whether or not the Web component hosts the Model Manager.

- Configure Java.
  - Install 64-bit Java 1.8 update 161 or later. Do not use 32-bit.

    The JRE is enough. You do not need the full JDK.
  - Set the JAVA_HOME environment variable to the Java installation folder.
  - Verify that `%JAVA_HOME%\bin\java.exe` is available.
- Configure Internet Information Services (IIS) according to the following table.

You need IIS 7.5 for Windows 2008 variants, IIS 8 for Windows 2012, IIS 8.5 for Windows 2012 R2, and IIS 10 for Windows 2016.

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

Table 2-6. IaaS Manager Service Host Internet Information Services

IIS Component	Setting
Internet Information Services (IIS) roles	■ Windows Authentication ■ Static Content ■ Default Document ■ ASPNET 3.5 and ASPNET 4.5 ■ ISAPI Extensions ■ ISAPI Filter
IIS Windows Process Activation Service roles	■ Configuration API ■ Net Environment ■ Process Model ■ WCF Activation (Windows 2008 variants only) ■ HTTP Activation ■ Non-HTTP Activation (Windows 2008 variants only) (Windows 2012 variants: Go to Features > .Net Framework 3.5 Features > Non-HTTP Activation)
IIS Authentication settings	Set the following non-defaults. ■ Windows Authentication enabled ■ Anonymous Authentication disabled Do not change the following defaults. ■ 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 variants

IaaS Manager Service Host

A Windows server that hosts the Manager Service component must meet additional requirements, in addition to those for all IaaS Windows servers.

The requirements are the same, whether the Manager Service host is a primary or backup.

- No firewalls can exist between a Manager Service host and DEM host. For port information, see IaaS Windows Server Ports.
- The Manager Service host must be able to resolve the NETBIOS name of the SQL Server database host. If it cannot resolve the NETBIOS name, add the SQL Server NETBIOS name to the Manager Service machine `/etc/hosts` file.

IaaS SQL Server Host

A Windows server that hosts the IaaS SQL database must meet certain requirements.

Your SQL Server can reside on one of your IaaS Windows servers, or on a separate host. When hosted together with IaaS components, these requirements are in addition to those for all IaaS Windows servers.

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

  If you create the database through the vRealize Automation installer, compatibility is already configured.
- AlwaysOn Availability Group (AAG) is only supported with SQL Server 2016 Enterprise. When you use AAG, you specify the AAG listener FQDN as the SQL Server host.
- When hosted together with IaaS components, configure Java.
  - Install 64-bit Java 1.8 update 161 or later. Do not use 32-bit.

    The JRE is enough. You do not need the full JDK.
  - Set the JAVA_HOME environment variable to the Java installation folder.
  - Verify that `%JAVA_HOME%\bin\java.exe` is available.
- Use a supported SQL Server version from the vRealize Automation Support Matrix.
- Enable TCP/IP protocol for SQL Server.
- SQL Server includes a model database that is the template for all databases created on the SQL instance. For IaaS to install correctly, do not change the model database size.
- Usually, the server needs more hardware than the minimums described in IaaS Windows Servers.

  For more information, see *Hardware Specifications and Capacity Maximums* in the vRealize Automation *Reference Architecture* guide.
- Before running the vRealize Automation installer, you need to identify accounts and add permissions in SQL. See Accounts and Passwords.

IaaS Distributed Execution Manager Host

A Windows server that hosts the Distributed Execution Manager (DEM) Orchestrator or Worker component must meet additional requirements, in addition to those for all IaaS Windows servers.

No firewalls can exist between a DEM host and Manager Service host. For port information, see IaaS Windows Server Ports.

DEM Workers might have additional requirements depending on the provisioning resources with which they interact.

DEM Workers with Amazon Web Services

A vRealize Automation IaaS DEM Worker that communicates with Amazon Web Services (AWS) must meet additional requirements, in addition to those for all IaaS Windows servers and DEMs in general.

A DEM Worker can communicate with AWS for provisioning. The DEM Worker communicates with, and collects data from, an Amazon EC2 account.

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

  Each URL resolves to a range of IP addresses, so you might need to use a tool, such as the one available from the Network Solutions Web site, to list and configure these IP addresses.
- If the DEM Worker reaches the Internet through a proxy server, the DEM service must be running under credentials that can authenticate to the proxy server.

DEM Workers with Openstack or PowerVC

A vRealize Automation IaaS DEM Worker that communicates with and collects data from Openstack or PowerVC must meet additional requirements, in addition to those for all IaaS Windows servers and DEMs in general.

Table 2-7. DEM Worker Openstack and PowerVC Requirements

Your Installation	Requirements
All	In Windows Registry, enable TLS v1.2 support for .NET framework. For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319
]
"SchUseStrongCrypto"=dword:00000001
```

Your Installation	Requirements
Windows 2008 DEM Host	In Windows Registry, enable TLS v1.2 protocol. For example:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.2]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
```

Your Installation	Requirements
Self-signed certificates on your infrastructure endpoint host	If your PowerVC or Openstack instance is not using trusted certificates, import the SSL certificate from your PowerVC or Openstack instance into the Trusted Root Certificate Authorities store on each IaaS Windows server where you intend to install a vRealize Automation DEM.

DEM Workers with Red Hat Enterprise Virtualization

A vRealize Automation IaaS DEM Worker that communicates with and collects data from Red Hat Enterprise Virtualization (RHEV) must meet additional requirements, in addition to those for all IaaS Windows servers and DEMs in general.

- You must join each RHEV environment to the domain containing the DEM Worker server.
- The credentials used to manage the endpoint representing an RHEV environment must have administrator privileges on the RHEV environment. When you use RHEV for provisioning, the DEM Worker communicates with and collects data from that account.
- The credentials must also have enough privileges to create objects on the hosts within the environment.

DEM Workers with SCVMM

A vRealize Automation IaaS DEM Worker that manages virtual machines through System Center Virtual Machine Manager (SCVMM) must meet additional requirements, in addition to those for all IaaS Windows servers and DEMs in general.

- Install the DEM Worker on the same machine with the SCVMM console.

  A best practice is to install the SCVMM console on a separate DEM Worker.

- The DEM worker must have access to the SCVMM PowerShell module installed with the console.
- The PowerShell Execution Policy must be set to RemoteSigned or Unrestricted.

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

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

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

vRealize Automation does not support a deployment environment that uses an SCVMM private cloud configuration. vRealize Automation cannot currently collect from, allocate to, or provision based on SCVMM private clouds.

The following additional requirements apply to SCVMM.

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

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

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

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

- Each SCVMM instance must be joined to the domain containing the server.
- The credentials used to manage the endpoint representing an SCVMM instance must have administrator privileges on the SCVMM server.

  The credentials must also have administrator privileges on the Hyper-V servers within the instance.

- To provision machines on an SCVMM resource, the vRealize Automation user who is requesting the catalog item must have the administrator role within the SCVMM instance.
- Hyper-V servers within an SCVMM instance to be managed must be Windows 2008 R2 SP1 Servers with Hyper-V installed. The processor must be equipped with the necessary virtualization extensions .NET Framework 4.5.2 or later must be installed and Windows Management Instrumentation (WMI) must be enabled.

- To provision a Generation-2 machine on an SCVMM 2012 R2 resource, you must add the following properties in the blueprint.

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

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

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

Certificates

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

For important information about troubleshooting, support, and trust requirements for certificates, see VMware Knowledge Base article 2106583.

Note vRealize Automation supports SHA2 certificates. The self-signed certificates generated by the system use SHA-256 With RSA Encryption. You might need to update to SHA2 certificates due to operating system or browser requirements.

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

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

Certificate Chains

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

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

- A root CA certificate

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

Certificate Changes if Customizing the vRealize Automation Login URL

If you want users to log in to a URL name other than a vRealize Automation appliance or load balancer name, see the pre and post installation CNAME steps in Set the vRealize Automation Login URL to a Custom Name.

vRealize Automation Certificate Requirements

When using your own certificates with vRealize Automation, the certificates need to meet certain requirements.

Supported Certificate Types

In many organizations, certificates are issued or requested by external authorities according to company requirements.

The following requirements address common identity format and certificate types used with typical vRealize Automation deployments.

Certificate Property	Requirements
Hash Algorithm	SHA1, SHA2, (256, 584, 512)
Signature Algorithm	RSASSA-PKCS1_V!_5
Key Length	2084, 4096

Note The RSASSA-PSS signature is not supported for vRealize Automation deployments. This signature is the default for a Microsoft CA on Windows 2012 R2. The signature is a configurable parameter, so you must ensure that it is set appropriately when using a Microsoft CA.

vRealize Automation Certificate Support Matrix

Hash Algorithm	SHA1				SHA2-256			
Signature Algorithm	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Key Size	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation Supported	Supported Verified	Supported Verified	Not Supported	Not Supported	Supported Verified	Supported Verified	Not Supported	Not Supported

Hash Algorithm	**SHA2-384**				**SHA2-512**			
Signature Algorithm	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Key Size	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation Supported	Supported Verified	Supported Verified	Not Supported	Not Supported	Supported Verified	Supported Verified	Not Supported	Not Supported

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)

Certificate Authority Provides	Command	Virtual Appliance Entries
RSA Private Key	openssl pkcs12 -in *path _to_.pfx certificate_file* -nocerts -out key.pem	**RSA Private Key**
PEM File	openssl pkcs12 -in *path _to_.pfx certificate_file* -clcerts -nokeys -out cert.pem	**Certificate Chain**
(Optional) Pass Phrase	n/a	**Pass Phrase**

Deploying the vRealize Automation Appliance

3

The vRealize Automation appliance is delivered as an open virtualization file that you deploy on existing virtualized infrastructure.

This chapter includes the following topics:

- About vRealize Automation Appliance Deployment
- Deploy the vRealize Automation Appliance
- Add Network Interface Controllers Before Running the Installer

About vRealize Automation Appliance Deployment

All installations first require a deployed but unconfigured vRealize Automation appliance, before you proceed with one of the actual vRealize Automation installation options.

- The consolidated, browser-based Installation Wizard
- Separate browser-based appliance configuration, followed by separate Windows installations for IaaS servers
- Command line based, silent installer that accepts input from an answer properties file
- The installation REST API that accepts JSON formatted input

Deploy the vRealize Automation Appliance

Before you can take any of the installation paths, vRealize Automation requires that you deploy at least one vRealize Automation appliance.

To create the appliance, you use the vSphere Client to download and deploy a partially configured virtual machine from a template. You might need to perform the procedure more than once, if you expect to create an enterprise deployment for high availability and failover. Such a deployment typically has multiple vRealize Automation appliances behind a load balancer.

Prerequisites

- Log in to the vSphere Client with an account that has permission to deploy OVF templates to the inventory.
- Download the vRealize Automation appliance `.ovf` or `.ova` file to a location accessible to the vSphere Client.

Procedure

1 Select the vSphere **Deploy OVF Template** option.

2 Enter the path to the vRealize Automation appliance `.ovf` or `.ova` file.

3 Review the template details.

4 Read and accept the end-user license agreement.

5 Enter an appliance name and inventory location.

  When you deploy appliances, use a different name for each one, and do not include non-alphanumeric characters such as underscores (_) in names.

6 Select the host and cluster in which the appliance will reside.

7 Select the resource pool in which the appliance will reside.

8 Select the storage that will host the appliance.

9 Select a disk format.

  Thick formats improve performance, and thin formats save storage space.

  Format does not affect appliance disk size. If an appliance needs more space for data, add disk by using vSphere after deploying.

10 From the drop-down menu, select a Destination Network.

11 Complete the appliance properties.

  a Enter and confirm a root password.

    The root account credentials log you in to the browser-based administration interface hosted by the appliance, or the appliance operating system command-line console.

  b Select whether or not to allow remote SSH connections to the command-line console.

    Disabling SSH is more secure but requires that you access the console directly in vSphere instead of through a separate terminal client.

c For **Hostname**, enter the appliance FQDN.

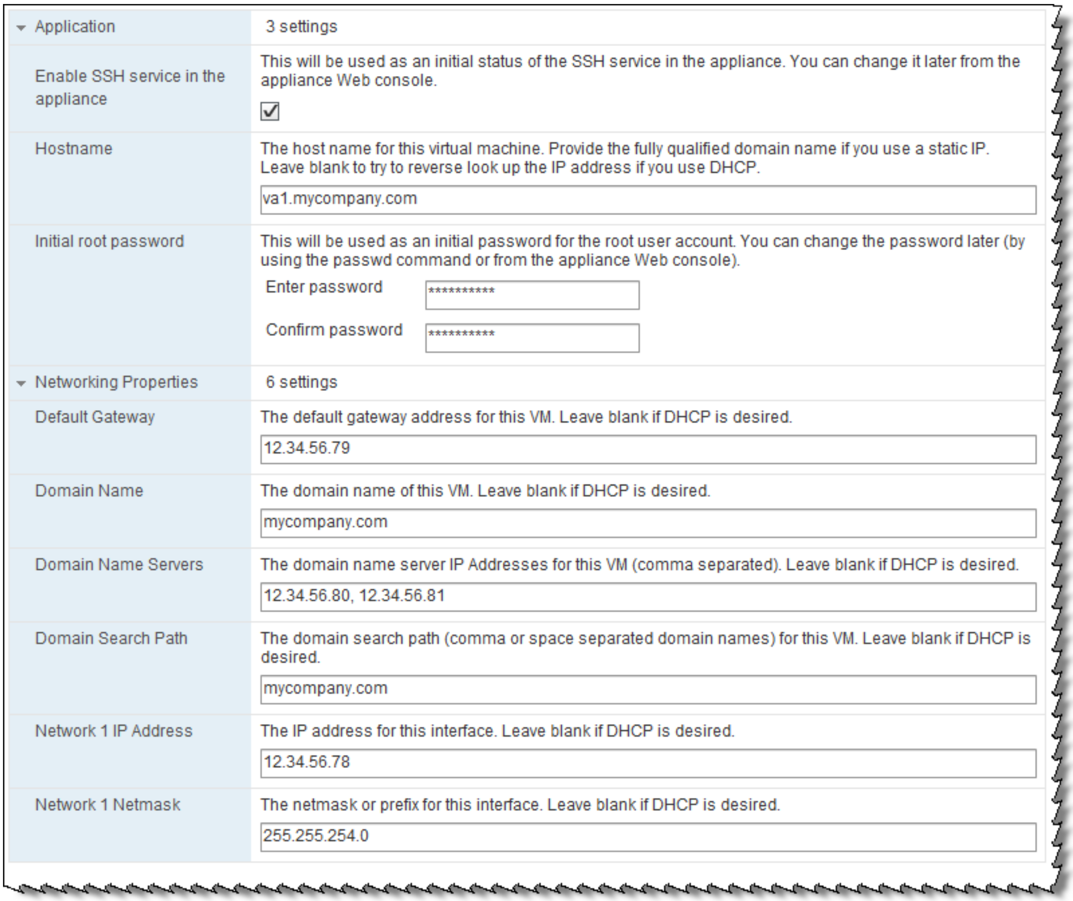
For best results, enter the FQDN even if using DHCP.

Note vRealize Automation supports DHCP, but static IP addresses are recommended for production deployments.

---

d In Network Properties, when using static IP addresses, enter the values for gateway, netmask, and DNS servers. You must also enter the IP address, FQDN, and domain for the appliance itself, as shown in the following example.

Figure 3-1. Example Virtual Appliance Properties



Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. ☑
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. va1.mycompany.com
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password ********** Confirm password **********
Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 12.34.56.79
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. mycompany.com
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. 12.34.56.80, 12.34.56.81
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. mycompany.com
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 12.34.56.78
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.254.0

12 Depending on your deployment, vCenter Server, and DNS configuration, select one of the following ways of finishing deployment and powering up the appliance.

- If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.

  a Select **Power on after deployment** and click **Finish**.

  b After the file finishes deploying into vCenter Server, click **Close**.

    c. Wait for the virtual machine to start, which might take up to 5 minutes.

- If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
    a. After the file finishes deploying into vCenter Server, click **Close**.
    b. Power on the vRealize Automation appliance.
    c. Wait for the virtual machine to start, which might take up to 5 minutes.
    d. Verify that the vRealize Automation appliance is deployed by pinging its FQDN. If you cannot ping the appliance, restart the virtual machine.
    e. Wait for the virtual machine to start, which might take up to 5 minutes.
- If you deployed the vRealize Automation appliance to vCloud using vCloud Director, vCloud might override the password that you entered during OVA deployment. To prevent the override, take the following steps.
    a. After deploying in vCloud Director, click your vApp to view the vRealize Automation appliance.
    b. Right-click the vRealize Automation appliance, and select **Properties**.
    c. Click the **Guest OS Customization** tab.
    d. Under **Password Reset**, clear the **Allow local administrator password** option, and click **OK**.
    e. Power on the vRealize Automation appliance.
    f. Wait for the virtual machine to start, which might take up to 5 minutes.

13. Verify that the vRealize Automation appliance is deployed by pinging its FQDN.

What to do next

- (Optional) Add NICs. See Add Network Interface Controllers Before Running the Installer.
- Log in to the browser-based administration interface to run the consolidated Installation Wizard or to manually configure the appliance.

  https://*vrealize-automation-appliance-FQDN*:5480
- Alternatively, you can skip logging in so that you can take advantage of vRealize Automation silent or API based installation.

Add Network Interface Controllers Before Running the Installer

vRealize Automation supports multiple network interface controllers (NICs). Before running the installer, it is possible to add NICs to the vRealize Automation appliance or IaaS Windows server.

If you need multiple NICs to be in place before running the vRealize Automation installation wizard, add them after deploying in vCenter but before starting the wizard. Reasons that you might want additional NICs in place early include the following examples:

- You want separate user and infrastructure networks.
- You need an additional NIC so that IaaS servers can join an Active Directory domain.

For more information about multiple NIC scenarios, see this VMware Cloud Management blog post.

For three or more NICs, be aware of the following limitations.

- VIDM needs access to the Postgres database and Active Directory.
- In an HA cluster, VIDM needs access to the load balancer URL.
- The preceding VIDM connections must come through the first two NICs.
- NICs after the second NIC must not be used or recognized by VIDM.
- NICs after the second NIC must not be used to connect to Active Directory.

  Use the first or second NIC when configuring a directory in vRealize Automation.

Prerequisites

Deploy the vRealize Automation appliance OVF and Windows virtual machines, but do not log in or start the installation wizard.

Procedure

1. In vCenter, add NICs to each vRealize Automation appliance.
   1. Right click the newly deployed appliance and select **Edit Settings**.
   2. Add VMXNETn NICs.
   3. If it is powered on, restart the appliance.
2. Log in to the vRealize Automation appliance command line as root.
3. Configure the NICs by running the following command for each NIC.

   Make sure to include the default gateway address. You can configure static routes after finishing this procedure.

   ```
   /opt/vmware/share/vami/vami_set_network network-interface (STATICV4|
   STATICV4+DHCPV6|STATICV4+AUTOV6) IPv4-address netmask gateway-v4-address
   ```

   For example:

   ```
   /opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20
   255.255.255.0 192.168.100.1
   ```
4. Verify that all vRealize Automation nodes can resolve each other by DNS name.
5. Verify that all vRealize Automation nodes can access any load balanced FQDNs for vRealize Automation components.

6 If you are using Split-Brain DNS, verify that all vRealize Automation nodes and VIPs have the same FQDN in DNS for each node IP and VIP.

7 In vCenter, add NICs to IaaS Windows servers.

   a Right click the IaaS server and select **Edit Settings**.

   b Add NICs to the IaaS server virtual machine.

8 In Windows, configure the added IaaS server NICs and their IP addresses. See the Microsoft documentation if necessary.

What to do next

- (Optional) If you need static routes, follow the guidelines in Configure Static Routes before continuing with installation.
- Log in to the browser-based administration interface to run the consolidated Installation Wizard or to manually configure the appliance.

  https://*vrealize-automation-appliance-FQDN*:5480
- Alternatively, you can skip logging in so that you can take advantage of vRealize Automation silent or API based installation.

Installing vRealize Automation with the Installation Wizard

4

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

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

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

The wizard is your primary tool for new vRealize Automation installations. If you want to expand an existing vRealize Automation deployment after running the wizard, see the procedures in Chapter 5 The Standard vRealize Automation Installation Interfaces.

This chapter includes the following topics:

Using the Installation Wizard for Minimal Deployments

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

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

Start the Installation Wizard for a Minimal Deployment

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

Prerequisites

- Address the prerequisites in Chapter 2 Preparing for vRealize Automation Installation.
- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.

Procedure

1. Log in as root to the vRealize Automation appliance administration interface.

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

2. When the Installation Wizard appears, click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Deployment Type page, select **Minimal deployment** and **Install Infrastructure as a Service**, and click **Next**.
5. On the Installation Prerequisites page, you pause to log in to your IaaS Windows server and install the Management Agent. The Management Agent allows the vRealize Automation appliance to discover and connect to the IaaS server.

What to do next

Install the Management Agent on your IaaS Windows server. See Install the vRealize Automation Management Agent.

Install the vRealize Automation Management Agent

All IaaS Windows servers require the Management Agent, which links them to their specific vRealize Automation appliance.

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

The Management Agent registers the IaaS Windows server with the specific 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 under a domain account with administrator rights on IaaS Windows servers.

Prerequisites

Create a vRealize Automation appliance and begin the Installation Wizard.

See Deploy the vRealize Automation Appliance and Start the Installation Wizard for a Minimal Deployment.

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
   ```

3. Copy the fingerprint so that you can verify it later. For example:

   ```
   71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
   ```

4. Log in to the IaaS Windows server using an account that has administrator rights.

5. Open a Web browser to the vRealize Automation appliance installer URL.

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

6. Click **Management Agent installer**, and save and run the `.msi` file.

7. Read the welcome.

8. Accept the end user license agreement.

9. Accept or change the installation folder.

   `Program Files (x86)\VMware\vCAC\Management Agent`

10. Enter vRealize Automation appliance details:

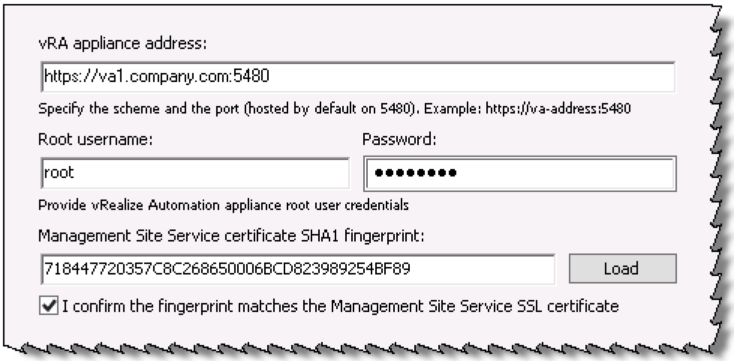
    a. Enter the appliance HTTPS address, including FQDN and :5480 port number.

    b. Enter the appliance root account credentials.

    c. Click **Load**, and confirm that the fingerprint matches the one you copied earlier. Ignore colons.

       If the fingerprints do not match, verify that you have the correct appliance address.

Figure 4-1. Management Agent—vRealize Automation Appliance Details



vRA appliance address:

https://va1.company.com:5480

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

Root username: root

Password: ●●●●●●●●●

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

718447720357C8C268650006BCD823989254BF89

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

11. Enter the domain\username and password for the service account.

    The service account must be a domain account with administrator rights on IaaS Windows servers. Use the same service account throughout.

12. Follow the prompts to finish installing the Management Agent.

Note Because they are linked, you must reinstall the Management Agent if you replace the vRealize Automation appliance.

Uninstalling IaaS from a Windows server does not remove the Management Agent. To uninstall a Management Agent, separately use the Add or Remove Programs option in Windows.

What to do next

Return to the browser-based Installation Wizard. IaaS Windows servers with the Management Agent installed appear under Discovered Hosts.

Completing the Installation Wizard

After installing the Management Agent, return to the wizard and follow the prompts. If you need additional instructions about settings, click the Help link at the upper right of the wizard.

- When you finish the wizard, the last page displays the path and name to a properties file. You can edit the file and use it to perform a silent vRealize Automation installation with the same or similar settings from your wizard session. See Chapter 6 Silent vRealize Automation Installation.
- If you created initial content, you can log in to the default tenant as the configurationadmin user and request the 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*.
- To configure access to the default tenant for other users, see Configure Access to the Default Tenant.

Using the Installation Wizard for Enterprise Deployments

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

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

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

Start the Installation Wizard for an Enterprise Deployment

Enterprise deployments are large enough for production environments. 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 deploy a distributed installation with load balancers, 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 Active Directory.

Prerequisites

- Address the prerequisites in Chapter 2 Preparing for vRealize Automation Installation.
- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.

Procedure

1 Log in as root to the vRealize Automation appliance administration interface.

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

2 When the Installation Wizard appears, click **Next**.

3 Accept the End User License Agreement and click **Next**.

4 On the Deployment Type page, select **Enterprise deployment** and **Install Infrastructure as a Service**.

5 On the Installation Prerequisites page, you pause to log in to your IaaS Windows servers and install the Management Agent. The Management Agent allows the vRealize Automation appliance to discover and connect to those IaaS servers.

What to do next

Install the Management Agent on your IaaS Windows servers. See Install the vRealize Automation Management Agent.

Install the vRealize Automation Management Agent

All IaaS Windows servers require the Management Agent, which links them to their specific vRealize Automation appliance.

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

The Management Agent registers the IaaS Windows server with the specific 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 under a domain account with administrator rights on IaaS Windows servers.

Prerequisites

Create a vRealize Automation appliance and begin the Installation Wizard.

See Deploy the vRealize Automation Appliance and Start the Installation Wizard for an Enterprise Deployment.

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
```

3 Copy the fingerprint so that you can verify it later. For example:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```

4 Log in to the IaaS Windows server using an account that has administrator rights.

5 Open a Web browser to the vRealize Automation appliance installer URL.

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

6 Click **Management Agent installer**, and save and run the `.msi` file.

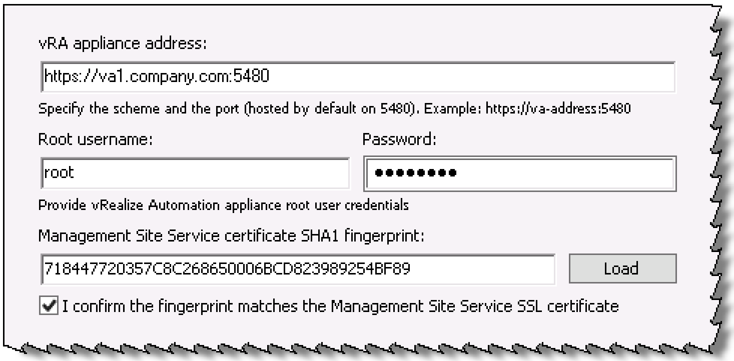
7 Read the welcome.

8. Accept the end user license agreement.
9. Accept or change the installation folder.

   `Program Files (x86)\VMware\vCAC\Management Agent`
10. Enter vRealize Automation appliance details:
    1. Enter the appliance HTTPS address, including FQDN and :5480 port number.
    2. Enter the appliance root account credentials.
    3. Click **Load**, and confirm that the fingerprint matches the one you copied earlier. Ignore colons.

       If the fingerprints do not match, verify that you have the correct appliance address.

       Figure 4-2. Management Agent—vRealize Automation Appliance Details

       vRA appliance address:

       https://va1.company.com:5480

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

       Root username: root

       Password: •••••••••

       Provide vRealize Automation appliance root user credentials

       Management Site Service certificate SHA1 fingerprint:

       718447720357C8C268650006BCD823989254BF89

       ☑ I confirm the fingerprint matches the Management Site Service SSL certificate
11. Enter the domain\username and password for the service account.

    The service account must be a domain account with administrator rights on IaaS Windows servers. Use the same service account throughout.
12. Follow the prompts to finish installing the Management Agent.

Repeat the procedure for all Windows servers that will host IaaS components.

Note Because they are linked, you must reinstall the Management Agent if you replace the vRealize Automation appliance.

Uninstalling IaaS from a Windows server does not remove the Management Agent. To uninstall a Management Agent, separately use the Add or Remove Programs option in Windows.

What to do next

Return to the browser-based Installation Wizard. IaaS Windows servers with the Management Agent installed appear under Discovered Hosts.

Completing the Installation Wizard

After installing the Management Agent, return to the wizard and follow the prompts. If you need additional instructions about settings, click the Help link at the upper right of the wizard.

- When you finish the wizard, the last page displays the path and name to a properties file. You can edit the file and use it to perform a silent vRealize Automation installation with the same or similar settings from your wizard session. See Chapter 6 Silent vRealize Automation Installation.
- If you created initial content, you can log in to the default tenant as the configurationadmin user and request the 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*.
- To configure access to the default tenant for other users, see Configure Access to the Default Tenant.

The Standard vRealize Automation Installation Interfaces

5

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

The Installation Wizard described in Chapter 4 Installing vRealize Automation with the Installation Wizard is your primary tool for new vRealize Automation installations. However, after you run the wizard, some operations still require the older, manual installation process.

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

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

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

This chapter includes the following topics:

Using the Standard Interfaces for Minimal Deployments

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

You install vRealize Automation in a minimal configuration for proof of concept or development work. Minimal deployments require fewer steps to install but lack the production capacity of an enterprise deployment.

Complete the high-level tasks in the following order.

Table 5-1. Minimal Deployment Checklist

	Task	Details
☐	Plan the environment and address installation prerequisites.	Chapter 2 Preparing for vRealize Automation Installation
☐	Create an unconfigured vRealize Automation appliance.	Deploy the vRealize Automation Appliance
☐	Manually configure the vRealize Automation appliance.	Configure the vRealize Automation Appliance
☐	Install IaaS components on a single Windows server.	Installing IaaS Components
☐	Install additional agents, if required.	Installing vRealize Automation Agents
☐	Perform post-installation tasks such as configuring the default tenant.	Configure Access to the Default Tenant

Configure the vRealize Automation Appliance

The vRealize Automation appliance is a partially configured virtual machine that hosts the vRealize Automation server and user web portal. You download and deploy the appliance open virtualization format (OVF) template to vCenter Server or ESX/ESXi inventory.

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Obtain an authentication certificate for the vRealize Automation appliance.

Procedure

1 Log in to the unconfigured vRealize Automation appliance management interface as root.

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

Continue past any certificate warnings.

2 If the installation wizard appears, cancel it so that you can go to the management interface instead of the wizard.

3 Select **Admin > Time Settings**, and set the time synchronization source.

Option	Description
Host Time	Synchronize to the vRealize Automation appliance ESXi host.
Time Server	Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.

You must synchronize vRealize Automation appliances and IaaS Windows servers to the same time source. Do not mix time sources within a vRealize Automation deployment.

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

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

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

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

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

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

If you want to generate a CSR request for a new certificate that you can submit to a certificate authority, select **Generate Signing Request**. A CSR helps your CA create a certificate with the correct values for you to import.

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.
Generate Signing Request	a Select **Generate Signing Request**. b Review the entries in the **Organization**, **Organization Unit**, **Country Code**, and **Common Name** text boxes. These entries are populated from the existing certificate. You can edit these entries if needed. c Click **Generate CSR** to generate a certificate signing request, and then click the **Download the generated CSR here** link to open a dialog that enables you to save the CSR to a location where you can send it to a certificate authority. d When you receive the prepared certificate, click **Import** and follow instructions for importing a certificate into vRealize Automation.
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.

6 Click **Save Settings** to save host information and SSL configuration.

7 Configure the SSO settings.

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

9 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).

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

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

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

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

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

11 Enter your license information.

   a Click **vRA Settings > Licensing**.

   b Click **Licensing**.

   c Enter a valid vRealize Automation license key that you downloaded when you downloaded the installation files, and click **Submit Key**.

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

12 Select whether to enable vRealize Code Stream and enter a vRealize Code Stream license.

   vRealize Code Stream is not supported for high-availability or production vRealize Automation deployments.

13 Confirm that you can log in to vRealize Automation.

   a Open a Web browser to the vRealize Automation product interface URL.

      https://*vrealize-automation-appliance-FQDN*/vcac

   b Accept the vRealize Automation certificate.

   c Accept the SSO certificate.

   d Log in with administrator@vsphere.local and the password you specified when you configured SSO.

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

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

What to do next

See Install the Infrastructure Components.

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 in the distributed deployment chapter.

Install the Infrastructure Components

The system administrator logs into the Windows machine and uses the installation wizard to install the IaaS services on the Windows virtual or physical machine.

Prerequisites

- Verify that the server meets the requirements in IaaS Windows Servers.
- Enable Time Synchronization on the Windows Server.
- Verify that you have deployed and fully configured the vRealize Automation appliance, and that the necessary services are running (plugin-service, catalog-service, iaas-proxy-provider).

Procedure

1. Download the vRealize Automation IaaS Installer

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

2. Select the Installation Type

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

3. Check Prerequisites

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

4. 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.

5. 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.

6. Register the IaaS Components

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

7. Finish the Installation

   The system administrator finishes the IaaS installation.

Download the vRealize Automation IaaS Installer

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

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

Prerequisites

- Review the IaaS Windows server requirements. See IaaS Windows Servers.
- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. Navigate to `res://iesetup.dll/SoftAdmin.htm` on the Windows server.

Procedure

1. Log in to the IaaS Windows server using an account that has administrator rights.
2. Open a Web browser directly to the vRealize Automation appliance installer URL.

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

   Do not change the installer file name. It is used to connect the installation to the vRealize Automation appliance.

Select the Installation Type

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

Prerequisites

Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next.**
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
5. Select **Accept Certificate**.
6. Click **Next**.

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

Check Prerequisites

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

Prerequisites

Select the Installation Type.

Procedure

1 Complete the Prerequisite Check.

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

2 Click **Next**.

The machine meets installation requirements.

Specify Server and Account Settings

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

Prerequisites

Check Prerequisites.

Procedure

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

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

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

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

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

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

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

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

5 Select the authentication method.

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

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

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

   By default, the checkbox is enabled. SSL provides a more secure connection between the IaaS server and SQL database. However, you must first configure SSL on the SQL server to support this option. For more about configuring SSL on the SQL server, see Microsoft Technet article 189067.

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.

Procedure

1 On the **Distributed Execution Managers And Proxy vSphere Agent** page, accept the defaults or change the names if appropriate.

2 Accept the default to install a vSphere agent to enable provisioning with vSphere or deselect it if applicable.

   a Select **Install and configure vSphere agent.**

   b Accept the default agent and endpoint, or type a name.

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

3 Click **Next**.

Register the IaaS Components

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

Prerequisites

Download the vRealize Automation IaaS Installer.

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.
- 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.

Using the Standard Interfaces for Distributed Deployments

Enterprise deployments are designed for greater vRealize Automation capacity in production and require that you distribute components across multiple machines. Enterprise deployments also might include redundant systems behind load balancers.

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 5-2. Distributed Deployment Checklist

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

vRealize Orchestrator

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

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

Directories Management

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

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

Disabling Load Balancer Health Checks

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

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

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

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

Certificate Trust Requirements in a Distributed Deployment

vRealize Automation uses certificates to maintain trust relationships and provide secure communication among components in distributed deployments.

In a distributed, or clustered, deployment, vRealize Automation certificate organization largely conforms to the three tiered architectural structure of vRealize Automation. The three tiers are vRealize Automation appliance, IaaS Website components, and Manager Service components. In a distributed system, each hardware machine in a particular tier shares a certificate. That is, each vRealize Automation appliance shares a common certificate, and each Manager Service machine shares the common certificate that applies to that layer.

You can use system or user generated self-signed certificates, or CA supplied certificates with distributed vRealize Automation deployments. Starting in vRealize Automation 7.0 and newer, if no certificates are supplied by the user, the installer automatically generates self-signed certificates for all applicable nodes and places them in the appropriate trust stores.

You can use load balancers with distributed vRealize Automation components to provide high availability and failover support. VMware recommends that vRealize Automation deployments use a pass-through configuration for deployments that use load balancers. In a pass-through configuration, load balancers pass requests along to the appropriate components rather than decrypting them. The vRealize Automation appliance and IaaS web servers must then perform the necessary decryption.

For more information about using and configuring load balancers, see *vRealize Automation Load Balancing*.

If you supply or generate your own certificates using Openssl or another tool, you can use either wildcard or Subject Alternative Name (SAN) certificates. Note that the IaaS certificates must be multi-use certificates.

If you are supplying certificates, you must obtain a multiple-use certificate that includes the IaaS component in the cluster, and then copy that certificate to the trust store for each component. If you use load balancers, you must include the load balancer FQDN in the trusted address of the cluster multiple-use certificate.

f you are need to update system generated self-signed certificates with user or CA supplied certificates, see *Managing vRealize Automation*.

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

Table 5-3. Certificate Trust Requirements

Import	Register
vRealize Automation appliance cluster	IaaS Web components cluster
IaaS Web component cluster	■ vRealize Automation appliance cluster ■ Manager Service components cluster ■ DEM Orchestrators and DEM Worker components
Manager Service component cluster	■ DEM Orchestrators and DEM Worker components ■ Agents and Proxy Agents

Configure Web Component, Manager Service and DEM Host Certificate Trust

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

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

Prerequisites

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

Procedure

1 Import the `web.pfx` and `ms.pfx` files to the following locations on the web component and manager service host machines:

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

2 Import the `web.pfx` and `ms.pfx` files to the following locations on the DEM Orchestrator and Worker host machines:

   Host Computer`/Certificates/Trusted People certificate store`

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

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

   a Select **Add/Remove Snap-in**.

   b Select **Certificates**.

   c Select **Local Computer**.

   d Open the certificate files that you imported previously and copy the thumb prints.

What to do next

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

Installation Worksheets

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

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

Table 5-4. vRealize Automation Appliance

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

Table 5-5. IaaS Windows Servers

Variable	My Value	Example
Primary IaaS Web Server with Model Manager Data FQDN		web.mycompany.com
Primary IaaS Web Server with Model Manager Data IP address For reference only; do not enter IP addresses		123.234.1.107
Additional IaaS Web Server FQDN		web2.mycompany.com
Additional IaaS Web Server IP address For reference only; do not enter IP addresses		123.234.1.108
IaaS Web Server load balancer FQDN		web-balance.mycompany.com

Table 5-5. IaaS Windows Servers (Continued)

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

Table 5-6. IaaS SQL Server Database

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

Table 5-7. IaaS Distributed Execution Managers

Variable	My Value	Example
DEM host FQDN		dem.mycompany.com
DEM host IP address For reference only; do not enter IP addresses		123.234.1.111
DEM host FQDN		dem2.mycompany.com

Table 5-7. IaaS Distributed Execution Managers (Continued)

Variable	My Value	Example
DEM host IP address For reference only; do not enter IP addresses		123.234.1.112
Unique DEM Orchestrator name		Orchestrator-1
Unique DEM Orchestrator name		Orchestrator-2
Unique DEM Worker name		Worker-1
Unique DEM Worker name		Worker-2
Unique DEM Worker name		Worker-3
Unique DEM Worker name		Worker-4

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. For information about extracting certificates, see Extracting Certificates and Private Keys
5. Configure the load balancer for vRealize Automation appliance traffic.
6. Configure the appliances for vRealize Automation. See Configuring Appliances for vRealize Automation.

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 more about load balancers, see the *vRealize Automation Load Balancing Configuration Guide* technical white paper.

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

Configuring Appliances for vRealize Automation

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

Configure the First vRealize Automation Appliance in a Cluster

The vRealize Automation appliance is a partially configured virtual machine that hosts the vRealize Automation server and user web portal. You download and deploy the appliance open virtualization format (OVF) template to vCenter Server or ESX/ESXi inventory.

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Obtain an authentication certificate for the vRealize Automation appliance.

  If your network or load balancer requires it, later procedures copy the certificate to the load balancer and additional appliances.

Procedure

1. Log in to the unconfigured vRealize Automation appliance management interface as root.

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

   Continue past any certificate warnings.
2. If the installation wizard appears, cancel it so that you can go to the management interface instead of the wizard.
3. Select **Admin > Time Settings**, and set the time synchronization source.

Option	Description
Host Time	Synchronize to the vRealize Automation appliance ESXi host.
Time Server	Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.

   You must synchronize all vRealize Automation appliances and IaaS Windows servers to the same time source. Do not mix time sources within a vRealize Automation deployment.

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

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

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

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

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

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

If you want to generate a CSR request for a new certificate that you can submit to a certificate authority, select **Generate Signing Request**. A CSR helps your CA create a certificate with the correct values for you to import.

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.

Option	Action
Generate Signing Request	a Select **Generate Signing Request**. b Review the entries in the **Organization**, **Organization Unit**, **Country Code**, and **Common Name** text boxes. These entries are populated from the existing certificate. You can edit these entries if needed. c Click **Generate CSR** to generate a certificate signing request, and then click the **Download the generated CSR here** link to open a dialog that enables you to save the CSR to a location where you can send it to a certificate authority. d When you receive the prepared certificate, click **Import** and follow instructions for importing a certificate into vRealize Automation.
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.

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 Select whether to enable vRealize Code Stream and enter a vRealize Code Stream license.

vRealize Code Stream is not supported for high-availability or production vRealize Automation deployments.

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

13 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).

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

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

14 Click **Save Settings.**

15 Confirm that you can log in to vRealize Automation.

   a Open a Web browser to the vRealize Automation product interface URL.

   https://*vrealize-automation-appliance-FQDN*/vcac

   b If prompted, continue past the certificate warnings.

   c Log in with administrator@vsphere.local and the password you specified when you configured SSO.

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

Configuring Additional Instances of the vRealize Automation Appliance

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

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

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

Add Another vRealize Automation Appliance to the Cluster

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

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

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

Prerequisites

- Have one or more vRealize Automation appliances already in the cluster, where one is the primary node. See Configure the First vRealize Automation Appliance in a Cluster.

  You can set a new appliance to be the primary node only after joining it to the cluster.
- Create the new appliance node. See Deploy the vRealize Automation Appliance.
- Verify that the load balancer is configured for use with the new appliance.
- Verify that traffic can pass through the load balancer to reach all current nodes and the new node that you are about to add.
- Verify that all vRealize Automation services are started on the current nodes.

Procedure

1. Log in to the new vRealize Automation appliance management interface as root.

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

   Continue past any certificate warnings.
2. If the installation wizard appears, cancel it so that you can go to the management interface instead of the wizard.
3. Select **Admin > Time Settings**, and set the time source to the same one that the rest of the cluster appliances use.

4 Select **vRA Settings > Cluster**.

5 Enter the FQDN of a previously configured vRealize Automation appliance in the **Leading Cluster Node** text box.

  You can use the FQDN of the primary vRealize Automation appliance, or any vRealize Automation appliance that is already joined to the cluster.

6 Type the root password in the **Password** text box.

7 Click **Join Cluster**.

8 Continue past any certificate warnings.

  Services for the cluster are restarted.

9 Verify that services are running.

  a Click the **Services** tab.

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

Disable Unused Services

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

Prerequisites

Add Another vRealize Automation Appliance to the Cluster

Procedure

1 Log in to the vRealize Automation appliance console.

2 Stop the vRealize Orchestrator service.

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

Validate the Distributed Deployment

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

Procedure

1 In the load balancer management interface or configuration file, temporarily disable all nodes except the node that you are testing.

2 Confirm that you can log in to vRealize Automation through the load balancer address:

  https://*vrealize-automation-appliance-load-balancer-FQDN*/vcac

3 After verifying that you can access the new vRealize Automation appliance through the load balancer, re-enable the other nodes.

Install the IaaS Components in a Distributed Configuration

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

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

Prerequisites

- Configure the First vRealize Automation Appliance in a Cluster.
- If your site includes multiple vRealize Automation appliances, Add Another vRealize Automation Appliance to the Cluster.
- Verify that the server meets the requirements in IaaS Windows Servers.
- 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

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

2. Download the vRealize Automation IaaS Installer

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

3. Choosing an IaaS Database Scenario

   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

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

5. Install Additional IaaS Web Server Components

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

6. Install the Active Manager Service

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

7 Install a Backup Manager Service Component

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

8 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.

9 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.

10 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.

What to do next

Install a DEM Orchestrator and at least one DEM Worker instance. See Installing Distributed Execution Managers.

Install IaaS Certificates

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

Prerequisites

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

Procedure

1 Obtain a certificate from a trusted certificate authority.

2 Open the Internet Information Services (IIS) Manager.

3 Double-click **Server Certificates** from Features View.

4 Click **Import** in the Actions pane.

   a Enter a file name in the **Certificate file** text box, or click the browse button **(…)**, to navigate to the name of a file where the exported certificate is stored.

   b Enter a password in the **Password** text box if the certificate was exported with a password.

   c Select **Mark this key as exportable**.

5 Click **OK**.

6 Click on the imported certificate and select **View**.

7 Verify that the certificate and its chain is trusted.

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

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

   ---

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

What to do next

Download the vRealize Automation IaaS Installer.

Download the vRealize Automation IaaS Installer

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

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

Prerequisites

- Configure the First vRealize Automation Appliance in a Cluster and, optionally, Add Another vRealize Automation Appliance to the Cluster.
- Verify that the server meets the requirements in IaaS Windows Servers.
- Verify that you imported a certificate to IIS and that the certificate root or the certificate authority is in the trusted root on the installation machine.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1 (Optional) Activate HTTP if you are installing on a Windows 2012 machine.

   a Select **Features > Add Features** from Server Manager.

   b Expand **WCF Services** under .NET Framework Features.

   c Select **HTTP Activation**.

2 Log in to the IaaS Windows server using an account that has administrator rights.

3 Open a Web browser directly to the vRealize Automation appliance installer URL. Do not use a load balancer address.

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

4 Click **IaaS Installer**.

5 Save `setup__vrealize-automation-appliance-FQDN@5480` to the Windows server.

   Do not change the installer file name. It is used to connect the installation to the vRealize Automation appliance.

6 Download the installer file to each IaaS Windows server on which you are installing components.

What to do next

Install an IaaS database, see Choosing an IaaS Database Scenario.

Choosing an IaaS Database Scenario

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

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

Note You can enable secure SSL when creating or upgrading the SQL database. For example, when you create or upgrade the SQL database, you can use the Secure SSL option to specify that the SSL configuration which is already specified in the SQL server be enforced when connecting to the SQL database. SSL provides a more secure connection between the IaaS server and SQL database. This option, which is available in the custom installation wizard, requires that you have already configured SSL on the SQL server. For related information about configuring SSL on the SQL server, see Microsoft Technet article 189067.

Table 5-8. Choosing an IaaS Database Scenario

Scenario	Procedure
Create the IaaS database manually using the provided database scripts. This option enables a database administrator to review the changes carefully before creating the database.	Create the IaaS Database Manually.
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.	Prepare an Empty Database.
Use the installer to create the database. This is the simplest option but requires the use of **sysadmin** privileges in the installer.	Create the IaaS Database Using the Installation Wizard.

Create the IaaS Database Manually

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

Prerequisites

- Install Microsoft .NET Framework 4.5.2 or later on the SQL Server host.
- Use Windows Authentication, rather than SQL Authentication, to connect to the database.
- Verify the database installation prerequisites. See IaaS SQL Server Host.

- Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.

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

Procedure

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

```
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 5-9. Database Values

Variable	Value
db_server	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`.
db_name	Name of the database. The default value is `vra`. Database names must consist of no more than 128 ASCII characters.
db_dir	Path to the data directory for the database, excluding the final slash.
log_dir	Path to the log directory for the database, excluding the final slash.
service_user	User name under which the Manager Service runs.
Web_user	User name under which the Web services run.
version_string	The vRealize Automation version, found by logging in to the vRealize Automation appliance and clicking the Update tab. For example, the vRealize Automation 6.1 version string is `6.1.0.1200`.

The database is created.

What to do next

Install the IaaS Components in a Distributed Configuration.

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 SQL Server Host.
- Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.

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

Procedure

1. Navigate to the `Database` directory 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 Windows database host with **sysadmin** privileges within the SQL Server instance.
4. Edit the following files, and replace all instances of the variables in the table with the correct values for your environment.

   ```
   CreateDatabase.sql
   SetDatabaseSettings.sql
   ```

   Table 5-10. Database Values

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

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

   The settings in the script are the recommended settings for the IaaS database. Only `ALLOW_SNAPSHOT_ISOLATION ON` and `READ_COMMITTED_SNAPSHOT ON` are required.
6. Open SQL Server Management Studio.

7 Click **New Query**.

   An SQL Query window opens.

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

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

10 Below the `CreateDatabase.sql` content, paste the entire modified contents of `SetDatabaseSettings.sql`.

11 Click **Execute**.

   The script runs and creates the database.

What to do next

Install the IaaS Components in a Distributed Configuration.

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.

Prerequisites

- If you are creating the database with Windows authentication, instead of SQL authentication, verify that the user who runs the installer has **sysadmin** rights on the SQL server.
- Download the vRealize Automation IaaS Installer.

Procedure

1 Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.

2 Click **Next**.

3 Accept the license agreement and click **Next**.

4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

    a. Type the user name, which is **`root`**, and the password.

        The password is the password that you specified when you deployed the vRealize Automation appliance.

    b. Select **Accept Certificate**.

    c. Click **View Certificate**.

        Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5. Click **Next**.

6. Select **Custom Install** on the Installation Type page.

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

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

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

    If you install more than one IaaS component, always install them to the same path.

9. Click **Next**.

10. On the IaaS Server Custom Install page, select **Database**.

11. In the **Database Instance** text box, specify the database instance or click **Scan** and select from the list of instances. If the database instance is on a non-default port, include the port number in instance specification by using the form *dbhost,SQL_port_number\SQLinstance*. The Microsoft SQL default port number is 1443.

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

    By default, the checkbox is enabled. SSL provides a more secure connection between the IaaS server and SQL database. However, you must first configure SSL on the SQL server to support this option. For more about configuring SSL on the SQL server, see Microsoft Technet article 189067.

13. Choose your database installation type from the **Database Name** panel.

    - Select **Use existing empty database** to create the schema in an existing database.
    - Enter a new database name or use the default name **`vra`** to create a new database. Database names must consist of no more than 128 ASCII characters.

14. Deselect **Use default data and log directories** to specify alternative locations or leave it selected to use the default directories (recommended).

15 Select an authentication method for installing the database from the **Authentication** list.

   - To use the credentials under which you are running the installer to create the database, select **User Windows identity....**
   - To use SQL authentication, deselect **Use Windows identity....** Type SQL credentials in the user and password text boxes.

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

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

16 Click **Next**.

17 Complete the Prerequisite Check.

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

18 Click **Install**.

19 When the success message appears, deselect **Guide me through initial configuration** and click **Next**.

20 Click **Finish**.

The database is ready for use.

Install an IaaS Website Component and Model Manager Data

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

Prerequisites

- Install the IaaS Database, see Choosing an IaaS Database Scenario.
- If you already installed other IaaS components, know the database passphrase that you created.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1. Install the First IaaS Web Server Component

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

2. Configure Model Manager Data

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

You can install additional Website components or install the Manager Service. See Install Additional IaaS Web Server Components or Install the Active Manager Service.

Install the First IaaS Web Server Component

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

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

Prerequisites

- Create the IaaS Database Using the Installation Wizard.
- Verify that the server meets the requirements in IaaS Windows Servers.
- If you already installed other IaaS components, know the database passphrase that you created.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

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

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

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

5 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

   a Type the user name, which is `root`, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

6 Click **Next**.

7 Select **Custom Install** on the Installation Type page.

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

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

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

   If you install more than one IaaS component, always install them to the same path.

10 Click **Next**.

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

12 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.

13 Type an available port number in the **Port number** text box, or accept the default port 443.

14 Click **Test Binding** to confirm that the port number is available for use.

15 Select the certificate for this component.

   a If you imported a certificate after you began the installation, click **Refresh** to update the list.

   b Select the certificate to use from **Available certificates**.

   c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

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

16 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.

17 (Optional) Select **Suppress certificate mismatch** to suppress certificate errors. The installation ignores certificate name mismatch errors as well as any remote certificate-revocation list match errors.

   This is a less secure option.

Configure Model Manager Data

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

Prerequisites

Install the First IaaS Web Server Component.

Procedure

1 Click the **Model Manager Data** tab.

2 In the **Server** text box, enter the vRealize Automation appliance fully qualified domain name.

   vrealize-automation-appliance.mycompany.com

   Do not enter an IP address.

3 Click **Load** to display the **SSO Default Tenant**.

   The `vsphere.local` default tenant is created automatically when you configure single sign-on. Do not modify it.

4 Click **Download** to import the certificate from the virtual appliance.

   It might take several minutes to download the certificate.

5 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.

6 Click **Accept Certificate**.

7 Enter **`administrator@vsphere.local`** in the **User name** text box and enter the password you created when you configured the SSO in the **Password** and **Confirm** text boxes.

8 (Optional) Click **Test** to verify the credentials.

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

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

   The default port is 443.

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

11 Click **Next**.

12 Complete the Prerequisite Check.

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

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

16 Click **Next**.

17 Click **Install**.

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

What to do next

You can install additional Web server components or install the Manager Service. See Install Additional IaaS Web Server Components or Install the Active Manager Service.

Install Additional IaaS Web Server Components

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

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

Prerequisites

- Install an IaaS Website Component and Model Manager Data.
- Verify that the new server meets the requirements in IaaS Windows Servers.
- Use the vRealize Automation appliance management interface to replace the certificate to include the FQDN of the new node. See *Replace Certificates in the vRealize Automation Appliance* in the *Managing vRealize Automation* guide.
- If you already installed other IaaS components, know the database passphrase that you created.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

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

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

2. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
3. Click **Next**.
4. Accept the license agreement and click **Next**.
5. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   1. 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.

   2. Select **Accept Certificate**.
   3. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

6. Click **Next**.
7. Select **Custom Install** on the Installation Type page.
8. Select **IaaS Server** under Component Selection on the Installation Type page.

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

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

   If you install more than one IaaS component, always install them to the same path.

10 Click **Next**.

11 Select **Website** on the **IaaS Server Custom Install** page.

12 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.

13 Type an available port number in the **Port number** text box, or accept the default port 443.

14 Click **Test Binding** to confirm that the port number is available for use.

15 Select the certificate for this component.

   a If you imported a certificate after you began the installation, click **Refresh** to update the list.

   b Select the certificate to use from **Available certificates**.

   c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

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

16 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.

17 (Optional) Select **Suppress certificate mismatch** to suppress certificate errors. The installation ignores certificate name mismatch errors as well as any remote certificate-revocation list match errors.

   This is a less secure option.

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

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

   The default port is 443.

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

20 Click **Next**.

21 Complete the Prerequisite Check.

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

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

25 Click **Next**.

26 Click **Install**.

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

What to do next

Install the Active Manager Service.

Install the Active Manager Service

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

Unless you enable automatic Manager Service failover, your IaaS deployment requires that only one Windows machine actively run the Manager Service at a time. Backup machines must have the service stopped and configured to start manually.

See About Automatic Manager Service Failover.

Prerequisites

- If you already installed other IaaS components, know the database passphrase that you created.
- (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.
- 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.

Procedure

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

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

2 Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.

3 Accept the license agreement and click **Next**.

4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

  a Type the user name, which is **`root`**, and the password.

    The password is the password that you specified when you deployed the vRealize Automation appliance.

  b Select **Accept Certificate**.

  c Click **View Certificate**.

    Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5 Click **Next**.

6 Select **Custom Install** on the Installation Type page.

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

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

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

  If you install more than one IaaS component, always install them to the same path.

9 Click **Next**.

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

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

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

The default port is 443.

12 Select **Active node with startup type set to automatic**.

13 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.

14 Type an available port number in the **Port number** text box, or accept the default port 443.

15 Click **Test Binding** to confirm that the port number is available for use.

16 Select the certificate for this component.

a If you imported a certificate after you began the installation, click **Refresh** to update the list.

b Select the certificate to use from **Available certificates**.

c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

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

17 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.

18 Click **Next**.

19 Check the prerequisites and click **Next**.

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

23 Click **Next**.

24 Click **Install**.

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

26 Click **Finish**.

What to do next

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

Install a Backup Manager Service Component

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

Unless you enable automatic Manager Service failover, your IaaS deployment requires that only one Windows machine actively run the Manager Service at a time. Backup machines must have the service stopped and configured to start manually.

See About Automatic Manager Service Failover.

Prerequisites

- If you already installed other IaaS components, know the database passphrase that you created.
- (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.

- Use the vRealize Automation appliance management interface to replace the certificate to include the FQDN of the new node. See *Replace Certificates in the vRealize Automation Appliance* in the *Managing vRealize Automation* guide.
- 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.

Procedure

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

   In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.
2. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
3. Click **Next**.
4. Accept the license agreement and click **Next**.
5. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   1. 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.
   2. Select **Accept Certificate**.
   3. Click **View Certificate**.

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

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

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

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

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

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

The default port is 443.

13 Select **Disaster recovery cold standby node**.

14 Select a Web site from available Web sites or accept the default Web site on the **Administration & Model Manager Web Site** tab.

15 Type an available port number in the **Port number** text box, or accept the default port 443.

16 Click **Test Binding** to confirm that the port number is available for use.

17 Select the certificate for this component.

  a If you imported a certificate after you began the installation, click **Refresh** to update the list.

  b Select the certificate to use from **Available certificates**.

  c If you imported a certificate that does not have a friendly name and it does not appear in the list, deselect **Display certificates using friendly names** and click **Refresh**.

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

18 (Optional) Click **View Certificate**, view the certificate, and click **OK** to close the information window.

19 Click **Next**.

20 Check the prerequisites and click **Next**.

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

24 Click **Next**.

25 Click **Install**.

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

27 Click **Finish**.

What to do next

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

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 IaaS Distributed Execution Manager Host.

Install the Distributed Execution Managers

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

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

Prerequisites

Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

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

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

   If you install more than one IaaS component, always install them to the same path.
9. Click **Next**.
10. Check prerequisites and click **Next**.

11 Enter the log in credentials under which the service will run.

The service account must have local administrator privileges and be the domain account that you have been using throughout IaaS installation. The service account has privileges on each distributed IaaS server and must not be a local system account.

12 Click **Next**.

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

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

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

The name cannot include spaces and cannot exceed 128 characters. If you enter a previously used name, the following message appears: "DEM name already exists. To enter a different name for this DEM, click Yes. If you are restoring or reinstalling a DEM with the same name, click No."

15 (Optional) Enter a description of this instance in **DEM description**.

16 Enter the host names and ports in the **Manager Service Host name** and **Model Manager Web Service Host name** text boxes.

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

The default port is 443.

17 (Optional) Click **Test** to test the connections to the Manager Service and Model Manager Web Service.

18 Click **Add**.

19 Click **Next**.

20 Click **Install**.

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

22 Click **Finish**.

What to do next

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

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

By default, the DEM Worker configuration file uses the default installation path of Microsoft System Center Virtual Machine Manager (SCVMM) console. You must update the file if you install the SCVMM console to a non-default location.

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

Prerequisites

- Know the non-default path where you installed the SCVMM console.

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

  `path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"`

Procedure

1. Stop the DEM Worker service.
2. Open the following file in a text editor.

   `Program Files (x86)\VMware\vCAC\Distributed Execution Manager\`*`instance-name`*`\DynamicOps.DEM.exe.config`
3. Locate the `<assemblyLoadConfiguration>` section.
4. Update each `path`, using the following example as a guideline.

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

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

For more information, see DEM Workers with SCVMM.

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

Configuring Windows Service to Access the IaaS Database

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

Enable IaaS Database Access from the Service User

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

Prerequisites

- Choosing an IaaS Database Scenario.
- Verify that the user name under which the Manager Service will run is not the owner of the database.

Procedure

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

   Do not replace `ServiceUser` in the line ending with `WHERE name = N'ServiceUser'`).
5. Open SQL Server Management Studio.
6. Select the database (vCAC by default) in **Databases** in the left-hand pane.
7. Click **New Query**.

   The SQL Query window opens in the right-hand pane.
8. Paste the modified contents of `VMPSOpsUser.sql` into the query window.
9. Click **Execute**.

Database access is enabled from the Manager Service.

Configure the Windows Services Account to Use SQL Authentication

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

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

Prerequisites

Verify that the vRealize Automation SQL Server database exists. Begin with Choosing an IaaS Database Scenario.

Procedure

1. Using an account with administrator privileges, log in to the IaaS Windows server that hosts the Manager Service.
2. In **Administrative Tools > Services**, stop the **VMware vCloud Automation Center** service.
3. Open the following files in a text editor.

   ```
   C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config
   ```

4. In each file, locate the `<connectionStrings>` section.
5. Replace

   `Integrated Security=True;`

   with

   `User Id=`*`database-username`*`;Password=`*`database-password`*`;`

6. Save and close the files.

   ```
   ManagerService.exe.config
   Web.config
   ```

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

Verify IaaS Services

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

Procedure

1. From the Windows desktop of the IaaS machine, select **Administrative Tools > Services.**

2 Locate the following services and verify that their status is Started and the Startup Type is set to Automatic.

   - VMware DEM – Orchestrator – *Name* where *Name* is the string provided in the **DEM Name** box during installation.
   - VMware DEM – Worker – *Name* where *Name* is the string provided in the **DEM Name** box during installation.
   - VMware vCloud Automation Center Agent *Agent name*
   - VMware vCloud Automation Center Service

3 Close the **Services** window.

Installing vRealize Automation Agents

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

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

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

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

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

For information about using vSphere agents, see vSphere Agent Requirements.

Set the PowerShell Execution Policy to RemoteSigned

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

For more information about the PowerShell Execution Policy, see the Microsoft PowerShell article about Execution Policies. If your PowerShell Execution Policy is managed at the group policy level, contact your IT support for about their restrictions on policy changes, and see the Microsoft PowerShell article about Group Policy Settings.

Prerequisites

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

Procedure

1. Using an administrator account, log in to the IaaS host machine where the agent is installed.
2. Select **Start > All Programs > Windows PowerShell version > Windows PowerShell**.
3. For Remote Signed, run `Set-ExecutionPolicy RemoteSigned`.
4. For Unrestricted, run `Set-ExecutionPolicy Unrestricted`.
5. Verify that the command did not produce any errors.
6. 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 5-11. Choosing an Agent Scenario

Integration Scenario	Agent Requirements and Procedures
Provision cloud machines by integrating with a cloud environment such as Amazon Web Services or Red Hat Enterprise Linux OpenStack Platform.	You do not need to install an agent.
Provision virtual machines by integrating with a vSphere environment.	Installing and Configuring the Proxy Agent for vSphere
Provision virtual machines by integrating with a Microsoft Hyper-V Server environment.	Installing the Proxy Agent for Hyper-V or XenServer
Provision virtual machines by integrating with a XenServer environment.	■ Installing the Proxy Agent for Hyper-V or XenServer ■ Installing the EPI Agent for Citrix
Provision virtual machines by integrating with a XenDesktop environment.	■ Installing the VDI Agent for XenDesktop ■ Installing the EPI Agent for Citrix
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
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
Provision virtual machines by integrating with any other supported virtual platform.	You do not need to install an agent.

Agent Installation Location and Requirements

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

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

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

Installing and Configuring the Proxy Agent for vSphere

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

vSphere Agent Requirements

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

Credentials

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

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

Table 5-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance

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

Table 5-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

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

Table 5-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

Attribute Value		Permission
		Deploy Template
		Read Customization Specs
	State	Create Snapshot
		Remove Snapshot
		Revert to Snapshot

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

Install the vSphere Agent

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

Prerequisites

- Install IaaS, including the Web server and Manager Service host.
- Verify that the machine where you install the agent is on a domain trusted by the domain where the IaaS components are installed.
- Verify that the requirements in vSphere Agent Requirements have been met.
- If you already created a vSphere endpoint for use with this agent, make a note of the endpoint name.
- Download the vRealize Automation IaaS Installer.

Procedure

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

4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

   a Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5 Select **Custom Install** on the Installation Type page.

6 In the Component Selection area, select **Proxy Agents**.

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

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

   If you install more than one IaaS component, always install them to the same path.

8 Click **Next**.

9 Log in with administrator privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.

10 Click **Next**.

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

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

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

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

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

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

16 Enter the name of the endpoint.

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

17 Click **Add**.

18 Click **Next**.

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

After several minutes a success message appears.

20 Click **Next**.

21 Click **Finish**.

22 Verify that the installation is successful.

23 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

Configure the vSphere Agent.

Configure the vSphere Agent

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

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

Prerequisites

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

Procedure

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

   `cd %SystemDrive%\Program Files (x86)\VMware\vCAC\Agents\agent-name`
3. (Optional) To view the current configuration settings, enter the following command.

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

   The following is an example of the command output.

   ```
   managementEndpointName: VCendpoint
   doDeletes: True
   ```
4. (Optional) To change the name of the endpoint that you configured at installation, use the following command.

   `set managementEndpointName`

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

   You use this process to rename the endpoint within vRealize Automation, instead of changing endpoints.
5. (Optional) To configure the virtual machine deletion policy, use the following command.

   `set doDeletes`

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

Option	Description
true	(Default) Delete virtual machines destroyed in vRealize Automation from vCenter Server.
false	Move virtual machines destroyed in vRealize Automation to the `VRMDeleted` directory in vCenter Server.
6. Open **Administrative Tools > Services** and restart the vRealize Automation Agent – *agent-name* service.

What to do next

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

Installing the Proxy Agent for Hyper-V or XenServer

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

Hyper-V and XenServer Requirements

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

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

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

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

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

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

Install the Hyper-V or XenServer Agent

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

Prerequisites

- Install IaaS, including the Web server and Manager Service host.
- Download the vRealize Automation IaaS Installer.
- Verify that Hyper-V Hypervisor proxy agents have system administrator credentials.
- Verify that the credentials under which to run the agent service have administrative access to the installation host.
- Verify that all XenServer or Hyper-V instances on the hosts to be managed by the agent have administrator-level credentials.

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

  vRealize Automation cannot communicate with or manage any node that is not identified by its fully qualified domain name within the Xen pool.

- Configure Hyper-V for remote management to enable Hyper-V server communication with vRealize Automation Hyper-V proxy agents.

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

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

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

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

   If you install more than one IaaS component, always install them to the same path.
8. Click **Next**.
9. Log in with administrator privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.

11 Select the agent from the **Agent type** list.

   - Xen
   - Hyper-V

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

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

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

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

13 Communicate the **Agent name** to the IaaS administrator who configures endpoints.

   To enable access and data collection, the endpoint must be linked to the agent that was configured for it.

14 Configure a connection to the IaaS Manager Service host.

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

   The default port is 443.

15 Configure a connection to the IaaS Web server.

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

   The default port is 443.

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

17 Enter the credentials of a user with administrative-level permissions on the managed server instance.

18 Click **Add**.

19 Click **Next**.

20 (Optional) Add another agent.

For example, you can add a Xen agent if you previously added the Hyper-V agent.

21 Click **Install** to begin the installation.

After several minutes a success message appears.

22 Click **Next**.

23 Click **Finish**.

24 Verify that the installation is successful.

What to do next

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

Configure the Hyper-V or XenServer Agent.

Configure the Hyper-V or XenServer Agent

A system administrator can modify proxy agent configuration settings, such as the deletion policy for virtualization platforms. You can use the proxy agent utility to modify the initial configurations that are encrypted in the agent configuration file.

Prerequisites

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

Procedure

1 Change to the agents installation directory, where *agent_name* is the directory containing the proxy agent, which is also the name under which the agent is installed.

`cd Program Files (x86)\VMware\vCAC Agents\`*`agent_name`*

2 View the current configuration settings.

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

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

```
Username: XSadmin
```

3 Enter the `set` command to change a property, where *property* is one of the options shown in the table.

`DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set` *property value*

If you omit *value*, the utility prompts you for a new value.

Property	Description
`username`	The username representing administrator-level credentials for the XenServer or Hyper-V server the agent communicates with.
`password`	The password for the administrator-level username.

4 Click **Start > Administrative Tools > Services** and restart the vRealize Automation Agent – *agentname* service.

Example: Change Administrator-Level Credentials

Enter the following command to change the administrator-level credentials for the virtualization platform specified during the agent installation.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

What to do next

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

Installing the VDI Agent for XenDesktop

vRealize Automation uses Virtual Desktop Integration (VDI) PowerShell agents to register the XenDesktop machines it provisions with external desktop management systems.

The VDI integration agent provides the owners of registered machines with a direct connection to the XenDesktop Web Interface. You can install a VDI agent as a dedicated agent to interact with a single Desktop Delivery Controller (DDC) or as a general agent that can interact with multiple DDCs.

XenDesktop Requirements

A system administrator installs a Virtual Desktop Infrastructure (VDI) agent to integrate XenDesktop servers into vRealize Automation.

You can install a general VDI agent to interact with multiple servers. If you are installing one dedicated agent per server for load balancing or authorization reasons, you must provide the name of the XenDesktop DDC server when installing the agent. A dedicated agent can handle only registration requests directed to the server specified in its configuration.

Consult the *vRealize Automation Support Matrix* on the VMware Web site for information about supported versions of XenDesktop for XenDesktop DDC servers.

Installation Host and Credentials

The credentials under which the agent runs must have administrative access to all XenDesktop DDC servers with which it interacts.

XenDesktop Requirements

The name given to the XenServer Host on your XenDesktop server must match the UUID of the Xen Pool in XenCenter. See Set the XenServer Host Name 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 thevCenter 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.

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

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in XenDesktop Requirements have been met.
- Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   1. 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.
   2. Select **Accept Certificate**.
   3. Click **View Certificate**.

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

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

   If you install more than one IaaS component, always install them to the same path.
9. Click **Next**.
10. Log in with administrator privileges for the Windows services on the installation machine.

    The service must run on the same installation machine.
11. Click **Next**.
12. Select **VdiPowerShell** from the **Agent type** list.

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

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

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

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

14 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

15 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

17 Select the **VDI version**.

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

19 Click **Add**.

20 Click **Next**.

21 Click **Install** to begin the installation.

After several minutes a success message appears.

22 Click **Next**.

23 Click **Finish**.

24 Verify that the installation is successful.

25 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

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

Installing the EPI Agent for Citrix

External provisioning Integration (EPI) PowerShell agents integrate Citrix external machines into the provisioning process. The EPI agent provides on-demand streaming of the Citrix disk images from which the machines boot and run.

The dedicated EPI agent interacts with a single external provisioning server. You must install one EPI agent for each Citrix provisioning server instance.

Citrix Provisioning Server Requirements

A system administrator uses External Provisioning Infrastructure (EPI) agents to integrate Citrix provisioning servers and to enable the use of Visual Basic scripts in the provisioning process.

Installation Location and Credentials

Install the agent on the PVS host for Citrix Provisioning Services instances. Verify that the installation host meets Citrix Agent Host Requirements 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.

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

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in Citrix Provisioning Server Requirements have been met.
- Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

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

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

   If you install more than one IaaS component, always install them to the same path.
8. Click **Next**.
9. Log in with administrator privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.

11 Select **EPIPowerShell** from the Agent type list.

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

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

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

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

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

16 Select the EPI type.

17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.

18 Click **Add**.

19 Click **Next**.

20 Click **Install** to begin the installation.

After several minutes a success message appears.

21 Click **Next**.

22 Click **Finish**.

23 Verify that the installation is successful.

24 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

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

Installing the EPI Agent for Visual Basic Scripting

A system administrator can specify Visual Basic scripts as additional steps in the provisioning process before or after provisioning a machine, or when deprovisioning a machine. You must install an External Provisioning Integration (EPI) PowerShell before you can run Visual Basic scripts.

Visual Basic scripts are specified in the blueprint from which machines are provisioned. Such scripts have access to all of the custom properties associated with the machine and can update their values. The next step in the workflow then has access to these new values.

For example, you could use a script to generate certificates or security tokens before provisioning and use them in machine provisioning.

To enable scripts in provisioning, you must install a specific type of EPI agent and place the scripts you want to use on the system on which the agent is installed.

When executing a script, the EPI agent passes all machine custom properties as arguments to the script. To return updated property values, you must place these properties in a dictionary and call a vRealize Automation function. A sample script is included in the scripts subdirectory of the EPI agent installation directory. This script contains a header to load all arguments into a dictionary, a body in which you can include your function(s), and a footer to return updated custom properties values.

Note You can install multiple EPI/VBScripts agents on multiple servers and provision using a specific agent and the Visual Basic scripts on that agent's host. If you need to do this, contact VMware customer support.

Visual Basic Scripting Requirements

A system administrator installs External Provisioning Infrastructure (EPI) agents to enable the use of Visual Basic scripts in the provisioning process.

The following table describes the requirements that apply to installing an EPI agent to enable the use of Visual Basic scripts in the provisioning process.

Table 5-13. EPI Agents for Visual Scripting

Requirement	Description
Credentials	Credentials under which the agent will run must have administrative access to the installation host.
Microsoft PowerShell	Microsoft PowerShell must be installed on the installation host prior to agent installation: The version required depends on the operating system of the installation host and might have been installed with that operating system. Visit http://support.microsoft.com for more information.
MS PowerShell Execution Policy	MS PowerShell Execution Policy must be set to **RemoteSigned** or **Unrestricted**. For information on PowerShell Execution Policy issue one of the following commands at Power-Shell command prompt:

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

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

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in Visual Basic Scripting Requirements have been met.
- Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5 Select **Custom Install** on the Installation Type page.

6 Select **Component Selection** on the Installation Type page.

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

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

If you install more than one IaaS component, always install them to the same path.

8 Click **Next**.

9 Log in with administrator privileges for the Windows services on the installation machine.

The service must run on the same installation machine.

10 Click **Next**.

11 Select **EPIPowerShell** from the Agent type list.

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

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

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

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

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

16 Select the EPI type.

17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.

18 Click **Add**.

19 Click **Next**.

20 Click **Install** to begin the installation.

After several minutes a success message appears.

21 Click **Next**.

22 Click **Finish**.

23 Verify that the installation is successful.

24 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

Installing the WMI Agent for Remote WMI Requests

A system administrator enables the Windows Management Instrumentation (WMI) protocol and installs the WMI agent on all managed Windows machines to enable management of data and operations. The agent is required to collect data from Windows machines, such as the Active Directory status of the owner of a machine.

Enable Remote WMI Requests on Windows Machines

To use WMI agents, remote WMI requests must be enabled on the managed Windows servers.

Procedure

1 In each domain that contains provisioned and managed Windows virtual machines, create an Active Directory group and add to it the service credentials of the WMI agents that execute remote WMI requests on the provisioned machines.

2 Enable remote WMI requests for the Active Directory groups containing the agent credentials on each Windows machine provisioned.

Install the WMI Agent

The Windows Management Instrumentation (WMI) agent enables data collection from Windows managed machines.

Prerequisites

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in Enable Remote WMI Requests on Windows Machines have been met.
- Download the vRealize Automation IaaS Installer.

Procedure

1. Right-click the `setup__`*`vrealize-automation-appliance-FQDN`*`@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is **`root`**, and the password.

      The password is the password that you specified when you deployed the vRealize Automation appliance.

   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

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

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

   If you install more than one IaaS component, always install them to the same path.
8. Click **Next**.
9. Log in with administrator privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.
11. Select **WMI** from the **Agent type** list.

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

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

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

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

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

16 Click **Add**.

17 Click **Next**.

18 Click **Install** to begin the installation.

After several minutes a success message appears.

19 Click **Next**.

20 Click **Finish**.

21 Verify that the installation is successful.

22 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

Silent vRealize Automation Installation

6

vRealize Automation includes options for scripted, silent installation from the command line, and API-based silent installation. Both approaches require that you prepare, in advance, the values that you would normally enter by hand during a conventional installation.

This chapter includes the following topics:

About Silent vRealize Automation Installation

vRealize Automation silent installation uses an executable that references a text-based answer file.

In the answer file, you preconfigure system FQDNs, account credentials, and other settings that you typically add throughout a conventional wizard-based or manual installation. Silent installation is useful for the following kinds of deployments.

- Deploying multiple, nearly identical environments
- Repeatedly redeploying the same environment
- Performing unattended installations
- Performing scripted installations

Perform a Silent vRealize Automation Installation

You can perform an unattended, silent vRealize Automation installation from the console of a newly deployed vRealize Automation appliance.

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Create or identify your IaaS Windows servers, and configure their prerequisites.
- Install the Management Agent on your IaaS Windows servers.

  You may install the Management Agent using the traditional `.msi` file download or the silent process described in Perform a Silent vRealize Automation Management Agent Installation.

Procedure

1 Log in to the vRealize Automation appliance console as root.

2 Navigate to the following directory.

```
/usr/lib/vcac/tools/install
```

3 Open the `ha.properties` answer file in a text editor.

4 Add entries specific to your deployment in `ha.properties`, and save and close the file.

Alternatively, you can save time by copying and modifying an `ha.properties` file from another deployment instead of editing the entire default file.

5 From the same directory, start the installation by running the following command.

```
vra-ha-config.sh
```

Installation might take up to an hour or more to complete, depending on the environment and size of the deployment.

6 (Optional) After installation finishes, review the log file.

```
/var/log/vcac/vra-ha-config.log
```

The silent installer does not save proprietary data to the log, such as passwords, licenses, or certificates.

Perform a Silent vRealize Automation Management Agent Installation

You can perform a command line based vRealize Automation Management Agent installation on any IaaS Windows server.

Silent Management Agent installation consists of a Windows PowerShell script in which you customize a few settings. After adding your deployment-specific settings, you can silently install the Management Agent on all of your IaaS Windows servers by running copies of the same script on each one.

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Create or identify your IaaS Windows servers, and configure their prerequisites.

Procedure

1. Log in to the IaaS Windows server using an account that has administrator rights.
2. Open a Web browser to the vRealize Automation appliance installer URL.

   https://*vrealize-automation-appliance-FQDN*:5480/installer
3. Right-click the link to the `InstallManagementAgent.ps1` PowerShell script file, and save it to the desktop or a folder on the IaaS Windows server.
4. Open `InstallManagementAgent.ps1` in a text editor.
5. Near the top of the script file, add your deployment-specific settings.
   - The vRealize Automation appliance URL

     https://*vrealize-automation-appliance-FQDN*:5480
   - vRealize Automation appliance root user account credentials
   - vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers
   - The folder where you want to install the Management Agent, `Program Files (x86)` by default
   - (Optional) The thumbprint of the PEM format certificate that you are using for authentication
6. Save and close `InstallManagementAgent.ps1`.
7. To silently install the Management Agent, double-click `InstallManagementAgent.ps1`.
8. (Optional) Verify that installation has finished by locating **VMware vCloud Automation Center Management Agent** in the Windows Control Panel list of Programs and Features, and in the list of Windows services that are running.

Silent vRealize Automation Installation Answer File

Silent vRealize Automation installations require that you prepare a text-based answer file in advance.

All newly deployed vRealize Automation appliances contain a default answer file.

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

To perform a silent installation, you must use a text editor to customize the settings in `ha.properties` to the deployment that you want to install. The following examples are a few of the settings and information that you must add.

- Your vRealize Automation or suite license key
- vRealize Automation appliance node FQDNs
- vRealize Automation appliance root user account credentials
- IaaS Windows server FQDNs that will act as Web nodes, Manager Service nodes, and so on
- vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers

- Load balancer FQDNs
- SQL Server database parameters
- Proxy agent parameters to connect to virtualization resources
- Whether the silent installer should attempt to correct missing IaaS Windows server prerequisites

  The silent installer can correct many missing Windows prerequisites. However, some configuration problems, such as not enough CPU, cannot be changed by the silent installer.

To save time, you can reuse and modify an `ha.properties` file that was configured for another deployment, one where the settings were similar. Also, when you install vRealize Automation non-silently through the Installation Wizard, the wizard creates and saves your settings in the `ha.properties` file. The file might be useful to reuse and modify for silently installing a similar deployment.

The wizard does not save proprietary settings to the `ha.properties` file, such as passwords, licenses, or certificates.

The vRealize Automation Installation Command Line

vRealize Automation includes a console-based, command line interface for performing installation adjustments that might be required after initial installation.

The command line interface (CLI) can run installation and configuration tasks that are no longer available through the browser-based interface after initial installation. CLI features include rechecking prerequisites, installing IaaS components, installing certificates, or setting the vRealize Automation host name to which users point their Web browser.

The CLI is also useful for advanced users who want to script certain operations. Some CLI functions are used by silent installation, so familiarity with both features reinforces your knowledge of vRealize Automation installation scripting.

vRealize Automation Installation Command-Line Basics

The vRealize Automation installation command-line interface includes top-level, basic operations.

The basic operations display vRealize Automation node IDs, run commands, report command status, or display the help information. To show these operations and their options at the console display, enter the following command without any options or qualifiers.

```
vra-command
```

Display Node IDs

You need vRealize Automation node IDs so that you can run commands against the correct target systems. To display node IDs, enter the following command.

```
vra-command list-nodes
```

Make note of node IDs before running commands against specific machines.

Run Commands

Most command-line functions involve running a command against a node in the vRealize Automation cluster. To run a command, use the following syntax.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

As shown in the preceding syntax, many commands require parameters, and parameter values, selected by the user.

Display Command Status

Some commands take a few moments or even longer to finish. To monitor the progress of a command that was entered, enter the following command.

```
vra-command status
```

The status command is especially valuable for monitoring a silent install, which can take a long time for large deployment sizes.

Display Help

To display help for all available commands, enter the following command.

```
vra-command help
```

To display help for a single command, enter the following command.

```
vra-command help command-name
```

vRealize Automation Installation Command Names

Commands give you console access to many vRealize Automation installation and configuration tasks that you might want to perform after initial installation.

Examples of available commands include the following functions.

- Adding another vRealize Automation appliance to an existing installation
- Setting the host name that users point a Web browser to when they access vRealize Automation
- Creating the IaaS SQL Server database
- Running the prerequisite checker against an IaaS Windows server
- Importing certificates

For a complete list of available vRealize Automation commands, log in to the vRealize Automation appliance console, and enter the following command.

```
vra-command help
```

The long list of command names and parameters is not reproduced in separate documentation. To use the list effectively, identify a command of interest, and narrow your focus by entering the following command.

```
vra-command help command-name
```

The vRealize Automation Installation API

The vRealize Automation REST API for installation gives you the ability to create purely software-controlled installations for vRealize Automation.

The installation API requires a JSON formatted version of the same entries that the CLI based installation obtains from the `ha.properties` answer file. The following guidelines familiarize you with how the API works. From there, you should be able to design programmatic calls to the API to install vRealize Automation.

- To access the API documentation, point a Web browser to the following vRealize Automation appliance page.

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

  You need an unconfigured vRealize Automation appliance. See Deploy the vRealize Automation Appliance.
- To experiment with the API based installation, locate and expand the following PUT command.

  ```
  PUT /vra-install
  ```
- Copy the unpopulated JSON from the **install_json** box to a text editor. Fill in the answer values the same way that you would for `ha.properties`. When your JSON formatted answers are ready, copy the code back to **install_json** and overwrite the unpopulated JSON.

  Alternatively, you can edit the following template JSON and copy the result to **install_json**.

  ```
  /usr/lib/vcac/tools/install/installationProperties.json
  ```

  You can also convert a completed `ha.properties` to JSON or vice versa.
- In the action box, select **validate** and click **Try It Out**.

  The validate action runs the vRealize Automation prerequisite checker and fixer.
- The validate response includes an alphanumeric command ID that you can insert into the following GET command.

  ```
  GET /commands/command-id/aggregated-status
  ```

  The response to the GET includes the progress of the validation operation.
- When validation succeeds, you can run the actual installation by repeating the process. In the action box, just select **install** instead of **validate**.

Installation can take a long time depending on the deployment size. Again, locate the command ID, and use the aggregated status GET command to obtain installation progress. The GET response might resemble the following example.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- If something goes wrong with the installation, you can trigger log collection for all nodes using the following command.

  ```
  PUT /commands/log-bundle
  ```

  Similar to installation, the returned alphanumeric command ID lets you monitor log collection status.

Convert Between vRealize Automation Silent Properties and JSON

For silent vRealize Automation CLI or API based installations, you can convert a completed properties answer file to JSON or vice versa. The silent CLI installation requires the properties file, while the API requires JSON format.

Prerequisites

A completed properties answer file or completed JSON file

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

or

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Procedure

1 Log in to a vRealize Automation appliance console session as root.

2 Run the appropriate converter script.

   - Convert JSON to Properties

     ```
     /usr/lib/vcac/tools/install/convert-properties --from-json
     installationProperties.json
     ```

     The script creates a new properties file with the timestamp in the name, for example:

     ```
     ha.2016-10-17_13.02.15.properties
     ```

   - Convert Properties to JSON

     ```
     /usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
     ```

     The script creates a new `installationProperties.json` file with the timestamp in the name, for example:

     ```
     installationProperties.2016-10-17_13.36.13.json
     ```

You can also display help for the script.

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

vRealize Automation Post-Installation Tasks

7

After you install vRealize Automation, there are post-installation tasks that might need your attention.

This chapter includes the following topics:

Configure Federal Information Processing Standard Compliant Encryption

You can enable or disable Federal Information Processing Standard (FIPS) 140–2 compliant cryptography for inbound and outbound vRealize Automation appliance network traffic.

Changing the FIPS setting requires a vRealize Automation restart. FIPS is disabled by default.

Procedure

1 Log in as root to the vRealize Automation appliance management interface.

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

2 Click **vRA Settings > Host Settings**.

3 Near the upper right, click the button to enable or disable FIPS.

   When enabled, inbound and outbound vRealize Automation appliance network traffic on port 443 uses FIPS 140–2 compliant encryption. Regardless of the FIPS setting, vRealize Automation uses AES–256 compliant algorithms to protect secured data stored on the vRealize Automation appliance.

   Note This vRealize Automation release only partially enables FIPS compliance, because some internal components do not yet use certified cryptographic modules. In cases where certified modules have not yet been implemented, the AES–256 compliant algorithms are used.

4 Click **Yes** to restart vRealize Automation.

You can also configure FIPS from a vRealize Automation appliance console session as root, using the following commands.

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

Enable Automatic Manager Service Failover

Automatic Manager Service failover is disabled by default if you install or upgrade the Manager Service with the standard vRealize Automation Windows installer.

To enable automatic Manager Service failover after running the standard Windows installer, take the following steps.

Procedure

1 Log in as root to a console session on the vRealize Automation appliance.

2 Navigate to the following directory.

   `/usr/lib/vcac/tools/vami/commands`

3 Enter the following command.

   `python ./manager-service-automatic-failover ENABLE`

If you need to disable automatic failover throughout an IaaS deployment, enter the following command instead.

`python ./manager-service-automatic-failover DISABLE`

About Automatic Manager Service Failover

You can configure the vRealize Automation IaaS Manager Service to fail over to a backup when the primary Manager Service stops.

Starting in vRealize Automation 7.3, you no longer have to manually start or stop the Manager Service on each Windows server, to control which serves as primary or backup. Automatic Manager Service failover is enabled by default in the following cases.

- When you install vRealize Automation silently or with the Installation Wizard.
- When you upgrade IaaS through the administration interface or with the automatic upgrade script.

Failover is not enabled when you use the standard Windows-based installer to add a Manager Service host or upgrade IaaS. To enable it, see Enable Automatic Manager Service Failover.

When automatic failover is enabled, the Manager Service automatically starts on all Manager Service hosts, including backups. The automatic failover feature allows hosts to transparently monitor each other and fail over when necessary. The feature requires that the Windows service is running on all hosts.

Note You are not required to use automatic failover. You may disable it and continue to manually start and stop the Windows service to control which host serves as primary or backup. If you take the manual failover approach, you must only start the service on one host at a time. With automatic failover disabled, simultaneously running the service on multiple IaaS servers makes vRealize Automation unusable.

Do not attempt to selectively enable or disable automatic failover. Automatic failover must always be synchronized as on or off, across every Manager Service host in an IaaS deployment.

If automatic failover does not appear to be working, see *Upgrading from vRealize Automation 7.1 or 7.2 to 7.3* for troubleshooting tips.

Automatic vRealize Automation PostgreSQL Database Failover

In a high availability vRealize Automation deployment, some configurations allow the embedded vRealize Automation PostgreSQL database to fail over automatically.

Automatic failover is silently enabled under the following conditions.

- The high availability deployment includes three vRealize Automation appliances.

  Automatic failover is not supported with only two appliances.
- Database replication is set to Synchronous Mode in vRA Settings > Database in the vRealize Automation administration interface.

Usually, you should avoid performing a manual failover while automatic failover is enabled. However, for some node problems, automatic failover might not occur even though it is enabled. When that happens, check to see if you need to perform a manual failover.

1. After the primary PostgreSQL database node fails, wait up to 5 minutes for the rest of the cluster to stabilize.
2. On a surviving vRealize Automation appliance node, open a browser to the following URL.

   https://*vrealize-automation-appliance-FQDN*:5434/api/status
3. Search for `manualFailoverNeeded`.

4 If `manualFailoverNeeded` is true, perform a manual failover.

For information about performing a manual failover, see *Managing vRealize Automation*.

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*.

Changing Host Names and IP Addresses

In general, you should expect to keep the host names, FQDNs, and IP addresses that you planned for vRealize Automation systems. Some post-installation changes are possible but can be complicated.

- If you change the host name of the Windows machine that hosts the IaaS SQL Server database, see *Managing vRealize Automation*.
- When restoring IaaS components, renaming a host can affect the IaaS Web host, Manager Service host, or their respective load balancers. Restore these hosts or load balancers according to the *vRealize Suite* backup and restore instructions.

To change a vRealize Automation appliance host name or IP address, see the following sections.

Change the vRealize Automation Appliance Host Name

When maintaining an environment or network, you might need to assign a different host name to a vRealize Automation appliance.

Important Renaming takes vRealize Automation offline for several minutes.

The same steps apply for standalone, master, and replica vRealize Automation appliances.

Procedure

1. In DNS, create an additional record with the new node host name.

   Do not remove the existing DNS record with the old host name yet.
2. Wait for DNS replication and zone distribution to occur.
3. Log in as root to the vRealize Automation appliance command line.
4. Run the following command.

   ```
   vcac-config hostname-change --host new-hostname --certificate certificate-file-name
   ```

   A certificate file is optional unless the old appliance host name was used in a certificate. If so, supply an updated certificate that has the new host name.

When you specify a certificate file, the renaming command also imports the certificate and returns the certificate ID.

A certificate file must be in the same format as the text output of the `/config/ssl/generate-certificate` API command and contain the new DNS name in its SAN field.

5. Wait up to 15 minutes or more for the renaming process to finish. The command actions take a few minutes, followed by several additional minutes for service re-registration.
6. If the old appliance host name was used with a load balancer in an HA environment, check and reconfigure the load balancer with the new name.
7. In DNS, remove the existing DNS record with the old host name.

If you have problems changing a host name, try the separate procedures from the vRealize Automation 7.3 documentation instead.

Change the vRealize Automation Appliance IP Address

When maintaining an environment or network, you might need to assign a different IP address to an existing vRealize Automation appliance.

Prerequisites

- As a precaution, take snapshots of vRealize Automation appliances and IaaS servers.
- From a console session as root on the vRealize Automation appliances, inspect entries in the `/etc/hosts` file.

  Look for address assignments that might conflict with the new IP address plan, and make changes as needed.

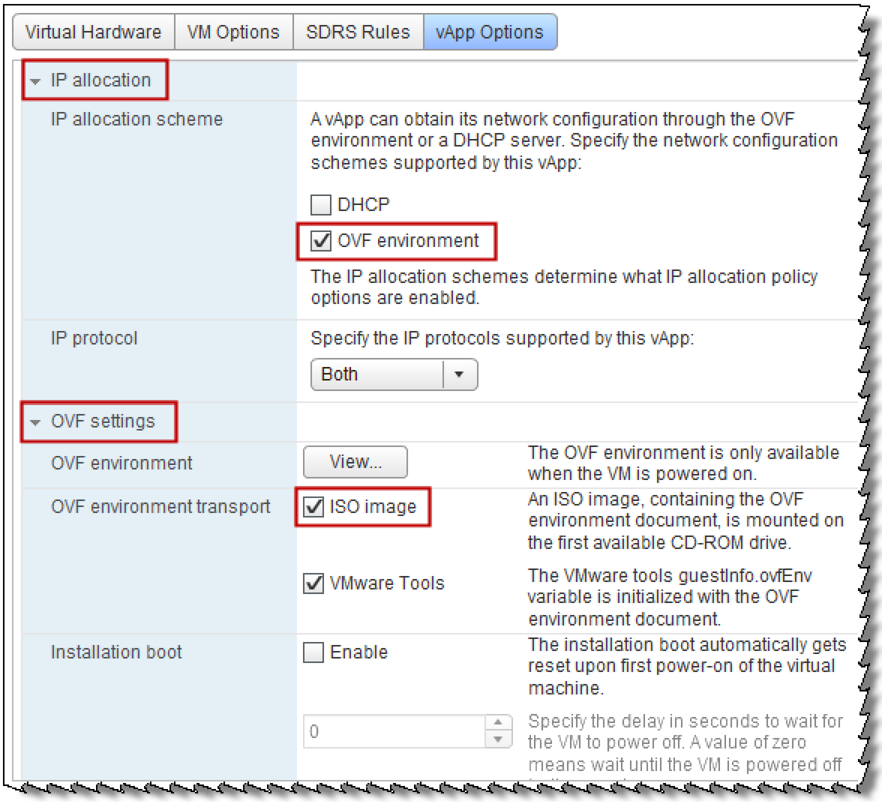
  On all IaaS servers, repeat the process for the `Windows\system32\drivers\etc\hosts` file.
- Shut down all vRealize Automation appliances.
- Stop all vRealize Automation services on IaaS servers.

Procedure

1. In vSphere, locate the vRealize Automation appliance that you want to change, and select **Actions > Edit Settings**.
2. Click **vApp Options**.
3. Expand **IP allocation**, and enable the **OVF environment** option.

4 Expand **OVF Settings**, and enable the **ISO image** option.

Figure 7-1. OVF Environment and ISO Image Options



IP allocation

IP allocation scheme: A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp:

☐ DHCP

☑ OVF environment

The IP allocation schemes determine what IP allocation policy options are enabled.

IP protocol: Specify the IP protocols supported by this vApp: Both

OVF settings

OVF environment: View... The OVF environment is only available when the VM is powered on.

OVF environment transport: ☑ ISO image An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive.

☑ VMware Tools The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document.

Installation boot: ☐ Enable The installation boot automatically gets reset upon first power-on of the virtual machine.

0 Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off

5 Click **OK**.

6 Start the vRealize Automation appliance that you are changing.

7 Log in as root to the vRealize Automation appliance management interface.

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

8 Click the **Network** tab.

9 Below the tabs, click **Address**.

10 Update the IP address.

11 At the upper right, click **Save Settings**.

12 Shut down the vRealize Automation appliance that you are changing.

13 In DNS, update entries for the new IP addresses.

Only update existing A-type records. Do not change FQDNs.

If using a load balancer, also update load balancer IP settings for back-end nodes, service pools, and virtual servers as needed.

14 Wait for DNS replication and zone distribution to occur.

15 Start all vRealize Automation appliances.

16 Start vRealize Automation services on IaaS servers.

17 Log in as root to the vRealize Automation appliance management interface.

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

18 Verify vRealize Automation appliance status in the following areas.

   - Database connection status under **vRA Settings** > **Database**
   - RabbitMQ status under **vRA Settings** > **Messaging**
   - Xenon status under **vRA Settings** > **Xenon**
   - All services as REGISTERED under **Services**

Adjusting the SQL Database for a Changed Host Name

You must revise configuration settings if you move the vRealize Automation IaaS SQL database to a different host name.

On the same host name, you can restore the SQL database from a backup with no further steps required. If you restore to a different host name, you need to edit configuration files to make additional changes.

See VMware Knowledge Base article 2074607 for the changes required when moving the SQL database to a different host name.

Change an IaaS Server IP Address

When maintaining an environment or network, you might need to assign a different IP address to an existing vRealize Automation IaaS Windows server.

Prerequisites

- If the vRealize Automation appliance IP address needs to change, do that first. See Change the vRealize Automation Appliance IP Address.
- As a precaution, take snapshots of vRealize Automation appliances and IaaS servers.
- From a console session as root on the vRealize Automation appliance, inspect entries in the `/etc/hosts` file.

  Look for address assignments that might conflict with the new IP address plan, and make changes as needed.

  On all IaaS servers, repeat the process for the `Windows\system32\drivers\etc\hosts` file.
- Shut down the vRealize Automation appliance.
- Stop all vRealize Automation services on IaaS servers.

Procedure

1 Log in to the IaaS server with an account that has administrator rights.

2 In Windows, change the IP address.

   Look for the IP address in the Windows network adapter settings, under Internet Protocol properties.

3 Refresh your local DNS with the changes.

   Refreshing DNS ensures that the IaaS Windows servers can find each other and that you can reconnect to a Windows server if you are disconnected.

4 On the Manager Service host, inspect the following file in a text editor.

   `install-folder\vCAC\Server\ManagerService.exe.config`

   The default install folder is `C:\Program Files (x86)\VMware`.

   Verify IP addresses or FQDNs of vRealize Automation appliances and IaaS Windows servers.

5 On all IaaS Windows servers, inspect the following file in a text editor.

   `install-folder\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

   Verify the IP address or FQDN of the vRealize Automation appliance.

6 Log in to the SQL Server host.

7 Verify that the repository address is correctly configured to use FQDN in the ConnectionString column.

   For example, open SQL Management Studio and run the following query.

   ```
   "SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].
   [Models]"
   ```

8 Start the vRealize Automation appliance.

9 Start vRealize Automation services on IaaS servers.

10 Inspect log files to verify that Agent, DEM Worker, Manager Service, and Web host services started successfully.

11 Log in to vRealize Automation as a user with the Infrastructure Administrator role.

12 Navigate to **Infrastructure > Monitoring > Distributed Execution Status** and verify that all services are running.

13 Test for correct operation by checking appliance services, testing provisioning, or using the vRealize Production Test tool.

Change an IaaS Server Host Name

When maintaining an environment or network, you might need to assign a different host name to an existing vRealize Automation IaaS Windows server.

Procedure

1 Take a snapshot of the IaaS server.

2 On the IaaS server, use IIS Manager to stop the vRealize Automation application pools: Repository, VMware vRealize Automation, and Wapi.

3 On the IaaS server, use Administrative Tools > Services to stop all vRealize Automation services, agents, and DEMs.

4 In DNS, create an additional record with the new host name.

Do not remove the existing DNS record with the old host name yet.

5 Wait for DNS replication and zone distribution to occur.

6 On the IaaS server, change the host name, but do not restart when prompted.

Look for the host name in the Windows system properties, under the computer name, domain, and workgroup settings.

When prompted to restart, click the option to restart later.

7 If you used the old host name to generate certificates, update certificates.

For information about updating certificates, see *Managing vRealize Automation*.

8 Use a text editor to locate and update the host name inside configuration files.

Make the updates based on which IaaS server host name you changed. In a distributed HA deployment, you might need to access more than one server. There are no updates if you change the host name of a DEM Orchestrator or DEM Worker.

Note Only update the old Windows server host name. If you find a load balancer name instead, keep the load balancer name.

Table 7-1. Files to Update When Changing a Web Node Host Name

IaaS Server	Path	File
Web nodes	*install-folder*\Server\Website	Web.config
	install-folder\Server\Website\Cafe	Vcac-Config.exe.config
	install-folder\Web API	Web.config
	install-folder\Web API\ConfigTool	Vcac-Config.exe.config
Node with the Model Manager component installed	*install-folder*\Server\Model Manager Data	Repoutil.exe.config
	install-folder\Server\Model Manager Data\Cafe	Vcac-Config.exe.config
Manager Service nodes	*install-folder*\Server	ManagerService.exe.config
DEM Orchestrator nodes	*install-folder*\Distributed Execution Manager\dem	DynamicOps.DEM.exe.config
DEM Worker nodes	*install-folder*\Distributed Execution Manager*DEM-name*	DynamicOps.DEM.exe.config

Table 7-1. Files to Update When Changing a Web Node Host Name (Continued)

IaaS Server	Path	File
Agent nodes	*install-folder*\Agents\agent-name	RepoUtil.exe.config
	install-folder\Agents\agent-name	VRMAgent.exe.config

Table 7-2. Files to Update When Changing a Manager Service Node Host Name

IaaS Server	Path	File
DEM Orchestrator nodes	*install-folder*\Distributed Execution Manager\DEM-name	DynamicOps.DEM.exe.config
DEM Worker nodes	*install-folder*\Distributed Execution Manager\dem	DynamicOps.DEM.exe.config
Agent nodes	*install-folder*\Agents\agent-name	VRMAgent.exe.config

Table 7-3. Files to Update When Changing an Agent Node Host Name

IaaS Server	Path	File
Agent node	*install-folder*\Agents\agent-name	VRMAgent.exe.config

9 Restart the IaaS server where you changed the host name.

10 Start the vRealize Automation application pools that you stopped earlier.

11 Start the vRealize Automation services, agents, and DEMs that you stopped earlier.

12 If the old IaaS server host name was used with a load balancer in an HA environment, check and reconfigure the load balancer with the new name.

13 In DNS, remove the existing DNS record with the old host name.

14 Wait for DNS replication and zone distribution to occur.

15 If you changed the host name of a Manager Service host, take the following additional steps.

  a Update software agents on existing virtual machines.

  b Recreate any ISOs or templates that contain a guest agent.

What to do next

Validate that vRealize Automation is ready for use. See the vRealize Suite Backup and Restore documentation.

Set the vRealize Automation Login URL to a Custom Name

If you want vRealize Automation users to log in to a URL name other than the vRealize Automation appliance or load balancer name, take customization steps before and after installation.

Procedure

1 Before installing, prepare a certificate that includes the CNAME that you want, as well as vRealize Automation appliance and load balancer names.

2 Install vRealize Automation, entering the appliance or load balancer name as usual. During installation, import the customized certificate.

3 After installing, in DNS, create a CNAME alias of Common Name, and point it to the appliance or load balancer VIP address.

4 Log in to the vRealize Automation appliance administrator interface as root.

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

5 Under **vRA Settings > Host Settings**, change the **Host Name** to the CNAME that you chose.

Licensing vRealize Code Stream

You can enable vRealize Code Stream by entering a vRealize Code Stream license in vRealize Automation.

You can enter the vRealize Code Stream license in either of these locations:

- On the Licensing page of the vRealize Automation installation wizard. For more information, see vRealize Code Stream Installation.
- On the Licensing tab in the vRealize Automation appliance management interface. For more information, see Apply a vRealize Code Stream License to an Appliance.

Installing the vRealize Log Insight Agent on IaaS Servers

The Windows servers in a vRealize Automation IaaS configuration do not include the vRealize Log Insight agent by default.

vRealize Log Insight provides log aggregation and indexing, and can collect, import, and analyze logs to expose system problems. If you want to capture and analyze logs from IaaS servers by using vRealize Log Insight, you must separately install the vRealize Log Insight agent for Windows.

For more information, see the *VMware vRealize Log Insight Agent Administration Guide*.

vRealize Automation appliances include the vRealize Log Insight agent by default.

Change the VMware Remote Console Proxy Port

If your site blocks or otherwise reserves port 8444, you can change the default proxy port used by VMware Remote Console.

Procedure

1 Access the vRealize Automation appliance command prompt as root.

2 Open the following file in a text editor.

   `/etc/vcac/security.properties`

3 Change `consoleproxy.service.port` from its default of 8444 to an unused port.

4 Save and close `security.properties`.

5 Restart the vRealize Automation appliance.

In an HA environment, make the same change to all vRealize Automation appliances.

Change a vRealize Automation Appliance FQDN Back to the Original FQDN

In some cases, a vRealize Automation appliance FQDN might change when you do not want it to. For example, the FQDN changes if you create an Integrated Windows Authentication (IWA) directory for a domain other than the domain that the appliance is on.

If you create an IWA directory for another domain, take the following steps to change the appliance FQDN back to the original FQDN.

Procedure

1. Log in to vRealize Automation and create the IWA directory as you normally would.

   See *Configuring vRealize Automation*.

2. If this is an HA environment, also follow the steps about configuring Directories Management for HA in *Configuring vRealize Automation*.

3. Creating an IWA directory for a domain other than the one that an appliance is on silently changes the appliance FQDN.

   For example, va1.domain1.local changes to va1.domain2.local when you create an IWA directory for domain2.local.

   Undo the change by renaming each appliance back to its original FQDN. See the associated procedure under Changing Host Names and IP Addresses.

4. After the appliances are completely back online with their original FQDN, log in to each IaaS node, and take the following steps.

   a Open the following file in a text editor.

   `C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

   b Change each appliance `endpoint address=` FQDN back to the original FQDN.

   For example, from:

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

To:

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

c Save and close `VMware.IaaS.Management.Agent.exe.Config`.

5. Log in as root to the vRealize Automation appliance management interface.

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

6. Go to **vRA settings** > **Messaging** and click **Reset RabbitMQ Cluster**.
7. After the reset finishes, log in to each appliance management interface.
8. Go to **vRA Settings** > **Cluster**, and verify that all nodes are connected to the cluster.

Configure SQL AlwaysOn Availability Group

You must make configuration changes if you set up SQL AlwaysOn Availability Group (AAG) after installing vRealize Automation.

When setting up SQL AAG after installation, follow the steps in VMware Knowledge Base article 2074607 to configure vRealize Automation with the AAG listener FQDN as the SQL Server host.

Add Network Interface Controllers After Installing vRealize Automation

vRealize Automation supports multiple network interface controllers (NICs). After installation, you can add NICs to the vRealize Automation appliance or IaaS Windows server.

Multiple NICs might be needed for some vRealize Automation deployments, for example:

- You want separate user and infrastructure networks.
- You need an additional NIC so that IaaS servers can join an Active Directory domain.

For more information about multiple NIC scenarios, see this VMware Cloud Management blog post.

For three or more NICs, be aware of the following limitations.

- VIDM needs access to the Postgres database and Active Directory.
- In an HA cluster, VIDM needs access to the load balancer URL.
- The preceding VIDM connections must come through the first two NICs.
- NICs after the second NIC must not be used or recognized by VIDM.
- NICs after the second NIC must not be used to connect to Active Directory.

  Use the first or second NIC when configuring a directory in vRealize Automation.

Prerequisites

Completely install vRealize Automation to your vCenter environment.

Procedure

1. In vCenter, add NICs to each vRealize Automation appliance.
   a. Right click the appliance and select **Edit Settings**.
   b. Add VMXNETn NICs.
   c. If it is powered on, restart the appliance.
2. Log in to the vRealize Automation appliance management interface as root.

   https://*vrealize-automation-appliance-FQDN*:5480
3. Select **Network**, and verify that multiple NICs are available.
4. Select **Address**, and configure the IP address for the NICs.

   Table 7-4. Example NIC Configuration

Setting	Value
IPv4 Address Type	Static
IPv4 Address	172.22.0.2
Netmask	255.255.255.0

5. Verify that all vRealize Automation nodes can resolve each other by DNS name.
6. Verify that all vRealize Automation nodes can access any load balanced FQDNs for vRealize Automation components.
7. If you are using Split-Brain DNS, verify that all vRealize Automation nodes and VIPs have the same FQDN in DNS for each node IP and VIP.
8. In vCenter, add NICs to IaaS Windows servers.
   a. Right click the IaaS server and select **Edit Settings**.
   b. Add NICs to the IaaS server virtual machine.
9. In Windows, configure the added IaaS server NICs and their IP addresses. See the Microsoft documentation if necessary.

What to do next

(Optional) If you need static routes, see Configure Static Routes.

Configure Static Routes

When adding NICs to a vRealize Automation installation, if you need static routes, you open a command prompt session to configure them.

Prerequisites

Add multiple NICs to vRealize Automation appliances or IaaS Windows servers.

Procedure

1 Log in to the vRealize Automation appliance command line as root.

2 Open the routes file in a text editor.

   `/etc/sysconfig/network/routes`

3 Locate the `default` line for the default gateway, but do not modify it.

   Note In cases where the default gateway needs to change, use the vRealize Automation management interface instead.

4 Below the `default` line, add new lines for static routes. For example:

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

5 Save and close the routes file.

6 Restart the appliance.

7 In HA clusters, repeat the process for each appliance.

8 Log in to the IaaS Windows server as an administrator.

9 Open a command prompt as administrator.

10 To configure a static route, enter the `route -p add` command, where `-p` persists the static route across restarts. For example:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

   For more information about configuring static routes in Windows, see the Microsoft documentation.

Access Patch Management

Technical support for your vRealize Automation installation might involve a software patch that you install or remove using the vRealize Automation appliance management interface.

Because issues can occur near real time, patches, prerequisites, and installation instructions are released in the VMware Knowledge Base. For example, VMware Knowledge Base article 56618 is monitored and updated with the latest vRealize Automation 7.4 patch information.

The patch interface cannot patch the following vRealize Automation components.

- The Management Agent
- Non vSphere agents such as XenServer, VDI, or Hyper-V

Procedure

1 Log in to the vRealize Automation appliance management interface as root.

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

2 Click **vRA Settings > Patches**.

3 Under Patch Management, click the option that you need, and follow the prompts.

Option	Description
New Patch	Install a new patch that you have downloaded.
Installed Patches	Add the most recently installed patch to newly added cluster nodes.
Rollback	Remove the most recently installed patch and roll vRealize Automation back to the previous patch level.
History	Inspect the list of installed and removed patches.

   To enable or disable Patch Management, log in to the vRealize Automation appliance command prompt as root, and enter one of the following commands.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Configure Access to the Default Tenant

You must grant your team access rights to the default tenant before they can begin configuring vRealize Automation.

The default tenant is automatically created when you configure single sign-on in the installation wizard. You cannot edit the tenant details, such as the name or URL token, but you can create new local users and appoint additional tenant or IaaS administrators at any time.

Procedure

1 Log in to vRealize Automation as the administrator of the default tenant.

   a Navigate to the vRealize Automation product interface.

      https://*vrealize-automation-FQDN*/vcac

   b Log in with the user name **`administrator`** and the password you defined for this user when you configured SSO.

2 Select **Administration > Tenants**.

3 Click the name of the default tenant, **vsphere.local**.

4 Click the **Local users** tab.

5. Create local user accounts for the vRealize Automation default tenant.

   Local users are tenant-specific and can only access the tenant in which you created them.

   a. Click the Add (+) icon.
   b. Enter details for the user responsible for administering your infrastructure.
   c. Click **Add**.
   d. Repeat this step to add one or more additional users who are responsible for configuring the default tenant.
6. Click the **Administrators** tab.
7. Assign your local users to the tenant administrator and IaaS administrator roles.
   a. Enter a username in the **Tenant administrators** search box and press Enter.
   b. Enter a username in the **IaaS administrators** search box and press Enter.

      The IaaS administrator is responsible for creating and managing your infrastructure endpoints in vRealize Automation. Only the system administrator can grant this role.
8. Click **Update**.

What to do next

Provide your team with the access URL and log in information for the user accounts you created so they can begin configuring vRealize Automation.

- Your tenant administrators configure settings such as user authentication, including configuring Directories Management for high availability. See *Configuring vRealize Automation*.
- Your IaaS administrators prepare external resources for provisioning. See *Configuring vRealize Automation*.
- If you configured Initial Content Creation during the installation, your configuration administrator can request the Initial Content catalog item to quickly populate a proof of concept. For an example of how to request the item and complete the manual user action, see *Installing and Configuring vRealize Automation for the Rainpole Scenario*.

Troubleshooting a vRealize Automation Installation

8

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
- Rolling Back a Failed Installation
- Create a vRealize Automation Support Bundle
- General Installation Troubleshooting
- Troubleshooting the vRealize Automation Appliance
- Troubleshooting IaaS Components
- Troubleshooting Log-In Errors

Default Log Locations

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

Note For log collection, consider taking advantage of the vRealize Automation and vRealize Orchestrator Content Packs for vRealize Log Insight. The Content Packs and Log Insight provide a consolidated summary of log events for components in the vRealize suite. For more information, visit the VMware Solution Exchange.

For the most recent log location list, see VMware Knowledge Base article 2141175.

Windows Logs

Use the following to find log files for Windows events.

Log	Location
Windows Event Viewer logs	**Start > Control Panel > Administrative Tools > Event Viewer**

Installation Logs

Installation logs are in the following locations.

Log	Default Location

Installation Logs	`C:\Program Files (x86)\vCAC\InstallLogs`
	`C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log`

WAPI Installation Logs	`C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>`

IaaS Logs

IaaS logs are in the following locations.

Log	Default Location
Website Logs	`C:\Program Files (x86)\VMware\vCAC\Server\Website\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`

   Note If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.
2. Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.
3. In IIS (Internet Information Services Manager) select Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).
4. Check that the Applications Repository, vRealize Automation and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.

The installation is completely removed.

Roll Back a Distributed Installation

A system administrator must manually remove some files and revert the database to completely uninstall a failed IaaS installation.

Procedure

1. If the following components are present, uninstall them with the Windows uninstaller.
   - vRealize Automation Server

- vRealize Automation WAPI

Note If you see the following message, restart the machine and then follow this procedure: `Error opening installation log file. Verify that the specified log file location exists and it is writable.`

Note If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.

2 Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.

3 In IIS (Internet Information Services Manager) select the Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).

4 Check that the Applications Repository, vCAC and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.

Table 8‑1. Roll Back Failure Points

Failure Point	Action
Installing Manager Service	If present, uninstall vCloud Automation Center Server.
Installing DEM-Orchestrator	If present, uninstall the DEM Orchestrator.
Installing DEM-Worker	If present, uninstall all DEM Workers.
Installing an Agent	If present, uninstall all vRealize Automation agents.

Create a vRealize Automation Support Bundle

You can create a vRealize Automation support bundle using the vRealize Automation appliance management interface. Support bundles gather logs, and help you or VMware technical support to troubleshoot vRealize Automation problems.

Procedure

1 Open a Web browser to the vRealize Automation appliance management interface URL.

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

2 Log in as root, and click **vRA Settings > Cluster**.

3 Click **Create Support Bundle**.

4 Click **Download** and save the support bundle file on your system.

Support bundles include information from the vRealize Automation appliance and IaaS Windows servers. If you lose connectivity between the vRealize Automation appliance and IaaS components, the support bundle might be missing the IaaS component logs.

To see which log files were collected, unzip the support bundle and open the `Environment.html` file in a Web browser. Without connectivity, IaaS components might appear in red in the Nodes table. Another reason that the IaaS logs are missing might be that the vRealize Automation management agent service has stopped on IaaS Windows servers that appear in red.

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.
2. Rerun the installation or upgrade.

Server Times Are Not Synchronized

An installation might not succeed when IaaS time servers are not synchronized with the vRealize Automation appliance.

Problem

You cannot log in after installation, or the installation fails while it is completing.

Cause

Time servers on all servers might not be synchronized.

Solution

Synchronize all vRealize Automation appliances and IaaS Windows servers to the same time source. Do not mix time sources within a vRealize Automation deployment.

- Set a vRealize Automation appliance time source:
    a. Log in to the vRealize Automation appliance management interface as root.

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

b Select **Admin > Time Settings**, and set the time synchronization source.

Option	Description
Host Time	Synchronize to the vRealize Automation appliance ESXi host.
Time Server	Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.

- For IaaS Windows servers, see Enable Time Synchronization on the Windows Server.

Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7

When you use Internet Explorer 9 or 10 on Windows 7 and compatibility mode is enabled, some pages appear to have no content.

Problem

When using Internet Explorer 9 or 10 on Windows 7, the following pages have no content:

- Infrastructure
- Default Tenant Folder on the Orchestrator page
- Server Configuration on the Orchestrator page

Cause

The problem could be related to compatibility mode being enabled. You can disable compatibility mode for Internet Explorer with the following steps.

Solution

Prerequisites

Ensure that the menu bar is displayed. If you are using Internet Explorer 9 or 10, press Alt to display the Menu bar (or right-click the Address bar and then select **Menu bar**).

Procedure

1. Select **Tools > Compatibility View settings**.
2. Deselect **Display intranet sites in Compatibility View**.
3. Click **Close**.

Cannot Establish Trust Relationship for the SSL/TLS Secure Channel

You might receive the message "Cannot establish trust relationship for the SSL/TLS secure channel when upgrading security certificates for vCloud Automation Center."

Problem

If a certificate issue occurs with vcac-config.exe when upgrading a security certificate, you might see the following message:

```
The underlying connection was closed: Could not establish trust relationship
for the SSL/TLS secure channel
```

You can find more information about the cause of the issue by using the following procedure.

Solution

1. Open `vcac-config.exe.config` in a text editor, and locate the repository address:

   `<add key="repositoryAddress" value="https://`*`IaaS-address`*`:443/repository/" />`

2. Open Internet Explorer to the address.
3. Continue through any error messages about certificate trust issues.
4. Obtain a security report from Internet Explorer, and use it to troubleshoot why the certificate is not trusted.

If problems persist, repeat the procedure by browsing with the address that needs to be registered, the Endpoint address that you used to register with `vcac-config.exe`.

Connect to the Network Through a Proxy Server

Some sites might connect to the Internet through a proxy server.

Problem

Your deployment cannot connect to the open Internet. For example, you cannot access Web sites, public clouds that you manage, or vendor addresses from which you download software or updates.

Cause

Your site connects to the Internet through a proxy server.

Solution

Prerequisites

Obtain proxy server names, port numbers, and credentials from the administrator for your site.

Procedure

1. Open a Web browser to the vRealize Automation appliance management interface URL.

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

2. Log in as root, and click **Network**.
3. Enter your site proxy server FQDN or IP address, and port number.
4. If your proxy server requires credentials, enter the user name and password.

5. Click **Save Settings**.

What to do next

Configuring to use a proxy might affect VMware Identity Manager user access. To correct the issue, see Proxy Prevents VMware Identity Manager User Log In.

Console Steps for Initial Content Configuration

There is an alternative to using the vRealize Automation installation interface to create the configuration administrator account and initial content.

Problem

As the last part of installing vRealize Automation, you follow the process to enter a new password, create the configurationadmin local user account, and create initial content. An error occurs, and the interface enters an unrecoverable state.

Solution

Instead of using the interface, enter console commands to create the configurationadmin user and initial content. Note that the interface might fail after successfully completing part of the process, so you might only need some of the commands.

For example, you might inspect logs and vRealize Orchestrator workflow execution, and determine that the interface-based setup created the configurationadmin user but not the initial content. In that case, you can enter just the last two console commands to complete the process.

Procedure

1. Log in to the vRealize Automation appliance console as root.
2. Import the vRealize Orchestrator workflow by entering the following command:

   ```
   /usr/sbin/vcac-config -e content-import --
   workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
   workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --
   tenant $TENANT
   ```

3. Execute the workflow to create the configurationadmin user:

   ```
   /usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workfl
   owexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
   password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-
   a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
   --tenant $TENANT
   ```

4. Import the ASD blueprint by entering the following command:

   ```
   /usr/sbin/vcac-config -e content-import --
   blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
   asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
   $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
   ```

5. Execute the workflow to configure initial content:

   ```
   /usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
   ```

Cannot Downgrade vRealize Automation Licenses

An error occurs when you submit the license key of a lower product edition.

Problem

You see the following message when using the vRealize Automation administration interface Licensing page to submit the key to a product edition that is lower than the current one. For example, you start with an enterprise license and try to enter an advanced license.

```
Unable to downgrade existing license edition
```

Cause

This vRealize Automation release does not support the downgrading of licenses. You can only add licenses of an equal or higher edition.

Solution

To change to a lower edition, reinstall vRealize Automation.

Troubleshooting the vRealize Automation Appliance

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using your vRealize Automation appliances.

Installers Fail to Download

Installers fail to download from the vRealize Automation appliance.

Problem

Installers do not download when running `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Cause

- Network connectivity issues when connecting to the vRealize Automation appliance machine.
- Not able to connect to the vRealize Automation appliance machine because the machine cannot be reached or it cannot respond before the connection times out.

Solution

1. Verify that you can connect to the vRealize Automation URL in a Web browser.

   https://*vrealize-automation-appliance-FQDN*

2 Check the other vRealize Automation appliance troubleshooting topics.

3 Download the setup file and reconnect to the vRealize Automation appliance.

Encryption.key File has Incorrect Permissions

A system error can result when incorrect permissions are assigned to the Encryption.key file for a virtual appliance.

Problem

You log in to vRealize Automation appliance and the Tenants page is displayed. After the page has begun loading, you see the message `System Error`.

Cause

The Encryption.key file has incorrect permissions or the group or owner user level is incorrectly assigned.

Solution

Prerequisites

Log in to the virtual appliance that displays the error.

Note If your virtual appliances are running under a load balancer, you must check each virtual appliance.

Procedure

1. View the log file `/var/log/vcac/catalina.out` and search for the message `Cannot write to /etc/vcac/Encryption.key`.
2. Go to the `/etc/vcac/` directory and check the permissions and ownership for the Encryption.key file. You should see a line similar to the following one:

   ```
   -rw------- 1 vcac vcac 48 Dec 4 06:48 encryption.key
   ```

   Read and write permission is required and the owner and group for the file must be `vcac`.
3. If the output you see is different, change the permissions or ownership of the file as needed.

What to do next

Log in to the Tenant page to verify that you can log in without error.

Directories Management Identity Manager Fails to Start After Horizon-Workspace Restart

In a vRealize Automation high availability environment, the Directories Management 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 might fail to start in a high availability environment because of issues with the liquibase data management utility used by vRealize Automation.

Solution

1 Log in as root to a console session on the vRealize Automation appliance.

2 Stop the horizon-workspace service by entering the following command.

```
#service horizon-workspace stop
```

3 Open the Postgres shell as super user.

```
su postgres
```

4 Navigate to the correct bin directory.

```
cd /opt/vmware/vpostgres/current/bin
```

5 Connect to the database.

```
psql vcac
```

6 From saas.databasechangeloglock, run the following SQL query.

```
select * from databasechangeloglock;
```

If the output shows a value of "t" for true, the lock must be released manually.

7 If you need to manually release the lock, run the following SQL query.

```
update saas.databasechangeloglock set locked=FALSE, lockgranted=NULL,
lockedby=NULL where id=1;
```

8 From saas.databasechangeloglock, run the following SQL query.

```
select * from databasechangeloglock;
```

The output should show a value of "f" for false, meaning it is unlocked.

9 Exit the Postgres vcac database.

```
vcac=# \q
```

10 Close the Postgres shell.

```
exit
```

11 Start the horizon-workspace service.

```
#service horizon–workspace start
```

Incorrect Appliance Role Assignments After Failover

After a failover occurs, master and replica vRealize Automation appliance nodes might not have the correct role assignment, which affects all services that require database write access.

Problem

In a high availability cluster of vRealize Automation appliances, you shut down or make the master database node inaccessible. You use the management console on another node to promote that node as the new master, which restores vRealize Automation database write access.

Later, you bring the old master node back online, but the Database tab in its management console still lists the node as the master node even though it is not. Attempts to use any node management console to clear the problem by officially promoting the old node back to master fail.

Solution

When failover occurs, follow these guidelines when configuring old versus new master nodes.

- Before promoting another node to master, remove the previous master node from the load balancer pool of vRealize Automation appliance nodes.
- To have vRealize Automation bring an old master node back to the cluster, let the old machine come online. Then, open the new master management console. Look for the old node listed as `invalid` under the Database tab, and click its **Reset** button.

  After a successful reset, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.
- To manually bring an old master node back to the cluster, bring the machine online, and join it to the cluster as if it were a new node. While joining, specify the newly promoted node as the primary node.

  After successfully joining, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.
- Until you correctly reset or rejoin an old master node to the cluster, do not use its management console for cluster management operations, even if the node came back online.
- After you correctly reset or rejoin, you may promote an old node back to master.

Failures After Promotion of Replica and Master Nodes

A disk space issue, along with the promotion of replica and master vRealize Automation appliance database nodes, might cause provisioning problems.

Problem

The master node runs out of disk space. You log in to its management interface Database page, and promote a replica node with enough space to become the new master. Promotion appears to succeed when you refresh the management interface page, even though an error message occurred.

Later, on the node that was the old master, you free up the disk space. After you promote the node back to master, however, provisioning operations fail by being stuck IN_PROGRESS.

Cause

vRealize Automation cannot properly update the old master node configuration when the problem is not enough space.

Solution

If the management interface displays errors during promotion, temporarily exclude the node from the load balancer. Correct the node problem, for example by adding disk, before re-including it on the load balancer. Then, refresh the management interface Database page and verify that the right nodes are master and replica.

Incorrect vRealize Automation Component Service Registrations

The vRealize Automation appliance management interface can help you resolve registration problems with vRealize Automation component services.

Problem

Under normal operation, all vRealize Automation component services must be unique and in a REGISTERED state. Any other set of conditions might cause vRealize Automation to behave unpredictably.

Cause

The following are examples of problems that might occur with vRealize Automation component services.

- A service has become inactive.
- Server settings caused a service to be in a state other than REGISTERED.
- A dependency on another service caused a service to be in a state other than REGISTERED.

Solution

Re-register component services that appear to have problems.

1 Take a snapshot of the vRealize Automation appliance.

   You might need to revert to the snapshot if you try different service changes, and the appliance ends up in an unpredictable state.

2 Log in to the vRealize Automation appliance management interface as root.

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

3 Click **Services**.

4 In the list of services, look for a service that is not in the correct state or has other problems.

5 If a faulty service is the `iaas-service`, go to the next step.

   Otherwise, to have vRealize Automation re-register the service, log in to a console session on the vRealize Automation appliance as root, and restart vRealize Automation by entering the following command.

   ```
   service vcac-server restart
   ```

   If there are services associated with the embedded vRealize Orchestrator instance, enter the following additional command.

   ```
   service vco-restart restart
   ```

6 If a faulty service is the `iaas-service`, take the following steps to re-register it.

   a Do not unregister the service.

   b On the primary IaaS Web Server, log in with an account that has Administrator rights.

   c Open a command prompt as Administrator.

   d Run the following command.

   ```
   "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
   ```

   The password is the administrator@vsphere.local password.

   e Run a command to update the registration information in the IaaS database.

   SQL Server with Windows Authentication:

   ```
   "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
   ```

   SQL Server with Native SQL Authentication:

   ```
   "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -sp SQL-user-password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
   ```

   To find the server or database name, inspect the following file in a text editor, and search for `repository`. Data Source and Initial Catalog values reveal the server address and database name, respectively.

`C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config`

The SQL user must have DBO privileges on the database.

f Register the endpoints by running the following commands:

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

g Register catalog items by running the following command:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-
Config.exe" RegisterCatalogTypesAsync -v
```

h Resart IIS.

`iisreset`

i Log in to the primary IaaS Manager Service host.

j Restart the vRealize Automation Windows service.

`VMware vCloud Automation Center Service`

7 To re-register any services associated with an external system, such as an external vRealize Orchestrator instance, log in to the external system and restart the services there.

Additional NIC Causes Management Interface Errors

After you add a second network interface card (NIC) to a vRealize Automation appliance, some vRealize Automation management interface pages fail to load properly.

Problem

You successfully add a second NIC using vCenter, and the following vRealize Automation management interface pages display errors instead of loading.

- The **Network > Status** page displays an error about an unresponsive script.
- The **Network > Address** page displays an error about failing to read network interface information.

Cause

Starting in version 7.3, the vRealize Automation appliance can support dual NICs. However, the engineering template on which the appliance is based prevents the management interface from working properly until you apply the solution.

Solution

After adding an additional NIC, restart the vRealize Automation appliance.

Cannot Promote a Secondary Virtual Appliance to Master

In vRealize Automation, low virtual appliance memory might prevent virtual appliance promotions in the cluster.

Problem

The master node runs low on memory. You log in to its management interface Database page, and try to promote a secondary node to become the new master. The following error occurs.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

Cause

Promotion only succeeds when all nodes can confirm reconfiguration to a newly promoted master. The low memory prevents the old master from confirming, even though all nodes are reachable.

Solution

Power off the master node that has low memory. Log in to the secondary node management interface Database page, and promote the secondary node.

Active Directory Sync Log Retention Time Is Too Short

In vRealize Automation, the Active Directory Sync logs go back only a couple days.

Problem

After two days, Active Directory Sync logs disappear from the management interface. Folders for the logs also disappear from the following vRealize Automation appliance directory.

`/db/elasticsearch/horizon/nodes/0/indices`

Cause

To conserve space, vRealize Automation sets the maximum retention time for Active Directory Sync logs to three days.

Solution

1 Log in to a console session on the vRealize Automation appliance as root.

2 Open the following file in a text editor.

   `/usr/local/horizon/conf/runtime-config.properties`

3 Increase the `analytics.maxQueryDays` property.

4 Save and close `runtime-config.properties`.

5 Restart the identity manager and elastic search services.

   ```
   service horizon-workspace restart
   service elasticsearch restart
   ```

RabbitMQ Cannot Resolve Host Names

RabbitMQ uses short host names for vRealize Automation appliances by default, which might prevent nodes from resolving one another.

Problem

You try to join another vRealize Automation appliance to the cluster, and an error similar to the following occurs.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
===========

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)


current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for
details.
```

Cause

Your network configuration does not allow vRealize Automation appliances to resolve each other by short host name.

Solution

1 For all vRealize Automation appliances in the deployment, log in as root to a console session.

2 Stop the RabbitMQ service.

```
service rabbitmq-server stop
```

3 Open the following file in a text editor.

```
/etc/rabbitmq/rabbitmq-env.conf
```

4 Set the following property to true.

```
USE_LONGNAME=true
```

5 Save and close `rabbitmq-env.conf`.

6 Reset RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

7 On just one vRealize Automation appliance node, run the following script.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

8 On all nodes, verify that the RabbitMQ service is started.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

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.

Prerequisite Fixer Cannot Install .NET Features

The vRealize Automation Prerequisite Checker **Fix** option fails and displays messages about not finding the installation source for .NET 3.5.1.

Problem

The Prerequisite Checker needs to verify that .NET 3.5.1 is installed in order to satisfy requirements for Windows Server 2008 R2 systems with IIS 7.5, and Windows Server 2012 R2 systems with IIS 8.

Cause

For Windows Server 2012 R2, inability to connect to the Internet can prevent .NET automatic installation. Certain Windows 2012 R2 updates can also prevent installation. The problem occurs because the Windows version lacks a local copy of the .NET Framework 3.5 installation source.

Solution

Manually provide a .NET Framework 3.5 installation source.

1 On the Windows host, mount an ISO of the Windows Server 2012 R2 installation media.

2 In Server Manager, enable .NET Framework 3.5 by using the Add Roles and Features Wizard.

3 During the wizard, navigate to the .NET Framework 3.5 installation path on the ISO media.

4 After adding .NET Framework 3.5, rerun the vRealize Automation Prerequisite Checker.

Validating Server Certificates for IaaS

You can use the vcac-Config.exe command to verify that an IaaS server accepts vRealize Automation appliance and SSO appliance certificates.

Problem

You see authorization errors when using IaaS features.

Cause

Authorization errors can occur when IaaS does not recognize security certificates from other components.

Solution

1. Open a command prompt as an administrator and navigate to the Cafe directory at `*vra-installation-dir*\Server\Model Manager Data\Cafe`, typically `C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe`.
2. Type a command of the form **`Vcac-Config.exe CheckServerCertificates -d [`*`vra-database`*`] -s [`*`vRA SQL server`*`] -v`**. Optional parameters are `-su [`*`SQL user name`*`]` and `-sp [`*`password`*`]`.

   If the command succeeds you see the following message:

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

   If the command fails, you see a detailed error message.

   Note This command is available only on the node for the Model Manager Data component.

Credentials Error When Running the IaaS Installer

When you install IaaS components, you get an error when entering your virtual appliance credentials.

Problem

After providing credentials in the IaaS installer, an `org.xml.sax.SAXParseException` error appears.

Cause

You used incorrect credentials or an incorrect credential format.

Solution

- Ensure that you use the correct tenant and user name values.

  For example, the SSO default tenant uses domain name such as vsphere.local, not administrator@vsphere.local.

Save Settings Warning Appears During IaaS Installation

Message appears during IaaS Installation. `Warning: Could not save settings to the virtual appliance during IaaS installation`.

Problem

An inaccurate error message indicating that user settings have not been saved appears during IaaS installation.

Cause

Communication or network problems can cause this message to appear erroneously.

Solution

Ignore the error message and proceed with the installation. This message should not cause the setup to fail.

Website Server and Distributed Execution Managers Fail to Install

Your installation of the vRealize Automation appliance infrastructure Web site 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 Web site 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

  Verify that you can connect to the vRealize Automation URL in a Web browser.

  https://*vrealize-automation-appliance-FQDN*
- Trusted Certificate Issues
  - In IaaS, open Microsoft Management Console with the command `mmc.exe` and check that the certificate used in the installation has been added to the Trusted Root Certificate Store in the machine.

  - From a Web browser, check the status of the MetaModel service and verify that no certificate errors appear:

    https://*FQDN-or-IP*/repository/data/MetaModel.svc

- Certificate Name Mismatch

  This error can occur when the certificate is issued to a particular name and a different name or IP address is used. You can suppress the certificate name mismatch error during installation by selecting **Suppress certificate mismatch**.

  You can also use the Suppress certificate mismatch option to ignore remote certificate revocation list match errors.

- Invalid Certificate

  Open Microsoft Management Console with the command `mmc.exe`. Check that the certificate is not expired and that the status is correct. Do this for all certificates in the certificate chain. You might have to import other certificates in the chain into the Trusted Root Certificate Store when using a Certificate hierarchy.

- Repository Service

  Use the following actions to check the status of the repository service.

  - From a Web browser, check the status of the MetaModel service:

    https://*FQDN-or-IP*/repository/data/MetaModel.svc

  - Check the `Repository.log` for errors.
  - Reset IIS (`iisreset`) if you have problems with the applications hosted on the Web site (Repository, vRealize Automation, or WAPI).
  - Check the Web site logs in *%SystemDrive%*`\inetpub\logs\LogFiles` for additional logging information.
  - Verify that Prerequisite Checker passed when checking the requirements.
  - On Windows 2012, check that WCF Services under .NET Framework is installed and that HTTP activation is installed.

IaaS Windows Servers Do Not Support FIPS

An installation cannot succeed when Federal Information Processing Standard (FIPS) is enabled.

Problem

Installation fails with the following error while installing the IaaS Web component.

```
This implementation is not part of the Windows Platform FIPS validated cryptographic
algorithms.
```

Cause

vRealize Automation IaaS is built on Microsoft Windows Communication Foundation (WCF), which does not support FIPS.

Solution

On the IaaS Windows server, disable the FIPS policy.

1. Go to **Start > Control Panel > Administrative tools > Local Security Policy**.
2. In the Group Policy dialog, under **Local Policies**, select **Security Options**.
3. Find and disable the following entry.

   `System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.`

Adding an XaaS Endpoint Causes an Internal Error

When you attempt to create an XaaS endpoint, an internal error message appears.

Problem

Creation of an endpoint fails with the following internal error message, `An internal error has occurred. If the problem persists, please contact your system administrator. When contacting your system administrator, use this reference:` *`c0DD0C01`*`.` Reference codes are randomly generated and not linked to a particular error message.

Solution

1. Open the vRealize Automation appliance log file.

   `/var/log/vcac/catalina.out`
2. Locate the reference code in the error message.

   For example, *c0DD0C01*.
3. Search for the reference code in the log file to locate the associated entry.
4. Review the entries that appear above and below the associated entry to troubleshoot the problem.

   The associated log entry does not specifically call out the source of the problem.

Uninstalling a Proxy Agent Fails

Removing a proxy agent can fail if Windows Installer Logging is enabled.

Problem

When you try to uninstall a proxy agent from the Windows Control Panel, the uninstall fails and you see the following error:

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

Cause

This can occur if Windows Installer Logging is enabled, but the Windows Installer engine cannot properly write the uninstallation log file. For more information, see Microsoft Knowledge Base article 2564571.

Solution

1 Restart your machine or restart explorer.exe from the Task Manager.

2 Uninstall the agent.

Machine Requests Fail When Remote Transactions Are Disabled

Machine requests fail when Microsoft Distributed Transaction Coordinator (DTC) remote transactions are disabled on Windows server machines.

Problem

If you provision a machine when remote transactions are disabled on the Model Manager portal or the SQL Server, the request will not complete. Data collection fails and the machine request remains in a state of CloneWorkflow.

Cause

DTC Remote Transactions are disabled in the IaaS SQL Instance used by the vRealize Automation system.

Solution

1 Launch Windows Server Manager to enable DTC on all vRealize servers and associated SQL servers.

   In Windows 7, navigate **Start > Administrative Tools > Component Services**.

   Note Ensure that all Windows servers have unique SIDs for MSDTC configuration.

   In addition, the IaaS Manager Service host must be able to resolve the NETBIOS name of the IaaS SQL Server database host. If it cannot resolve the NETBIOS name, add the SQL Server NETBIOS name to the Manager Service machine `/etc/hosts` file and restart the Manager Service.

2 Open all nodes to locate the local DTC, or the clustered DTC if using a clustered system.

   Navigate **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

3 Right click on the local or clustered DTC and select **Properties**.

4 Click the Security tab.

5 Select the **Network DTC Access** option.

6 Select the **Allow Remote Client** and **Allow Remote Administration** options.

7 Select the **Allow Inbound** and **Allow Outbound** options.

8 Enter or select NT AUTHORITY\Network Service in the **Account** field for the DTC Logon Account.

9 Click **OK**.

10 Remove machines that are stuck in the Clone Workflow state.

   a Log in to the vRealize Automation product interface.

   https://*vrealize-automation-appliance-FQDN*/vcac/org/*tenant-name*

   b Navigate to **Infrastructure > Managed Machines**.

   c Right click the target machine.

   d Select **Delete** to remove the machine.

Error in Manager Service Communication

IaaS servers cloned from a template where DTC was already installed contain duplicate identifiers for DTC, which prevents communication among the nodes.

Problem

The IaaS Manager Service fails and posts the following error to 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 server that already has DTC installed, the clone contains the same unique identifier for DTC as the parent. Communication between the two machines fails.

Solution

1 On the clone, open a command prompt as Administrator.

2 Run the following command.

   `msdtc -uninstall`

3 Restart the clone.

4 Open another command prompt, and run the following command.

   msdtc -install *manager-service-host-FQDN*

Email Customization Behavior Has Changed

In vRealize Automation 6.0 or later, only notifications generated by the IaaS component can be customized by using the email template functionality from earlier versions.

Solution

You can use the following XSLT templates:

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

Email templates are located in the `\Templates` directory under the server installation directory, typically `%SystemDrive%\Program Files x86\VMware\vCAC\Server`. The `\Templates` directory also includes XSLT templates that are no longer supported and cannot be modified.

Troubleshooting Log-In Errors

The troubleshooting topics for log-in errors for vRealize Automation provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Attempts to Log In as the IaaS Administrator with Incorrect UPN Format Credentials Fails with No Explanation

You attempt to log in to vRealize Automation as an IaaS administrator and are redirected to the login page with no explanation.

Problem

If you attempt to log in to vRealize Automation as an IaaS administrator with UPN credentials that do not include the *@yourdomain* portion of the user name, you are logged out of SSO immediately and redirected to the login page with no explanation.

Cause

The UPN entered must adhere to a *yourname*.admin@*yourdomain* format, for example if you log in using jsmith.admin@sqa.local as the user name but the UPN in the Active Directory is only set as jsmith.admin, the login fails.

Solution

To correct the problem change the `userPrincipalName` value to include the needed @*yourdomain* content and retry login. In this example the UPN name should be jsmith.admin@sqa.local. This information is provided in the log file in the `log/vcac` folder.

Log In Fails with High Availability

When you have more than one vRealize Automation appliance, the appliances must be able to identify each other by short hostname. Otherwise, you cannot log in.

Problem

You configure vRealize Automation for high availability by installing an additional vRealize Automation appliance. When you try to log in to vRealize Automation, a message about an invalid license appears. The message is incorrect though, because you determined that your license is valid.

Cause

The vRealize Automation appliance nodes do not correctly form a high availability cluster until they can resolve the short host names of the nodes in the cluster.

Solution

To allow a cluster of high availability vRealize Automation appliances to resolve short host names, take any of the following approaches. You must modify all appliances in the cluster.

Procedure

- Edit or create a search line in `/etc/resolv.conf`. The line should contain domains that hold vRealize Automation appliances. Separate multiple domains with spaces. For example:

  `search sales.mycompany.com support.mycompany.com`

- Edit or create domain lines in `/etc/resolv.conf`. Each line should contain a domain that holds vRealize Automation appliances. For example:

  `domain support.mycompany.com`

- Add lines to the `/etc/hosts` file so that each vRealize Automation appliance short name is mapped to its fully qualified domain name. For example:

  ```
  node1    node1.support.mycompany.com
  node2    node2.support.mycompany.com
  ```

Proxy Prevents VMware Identity Manager User Log In

Configuring to use a proxy might prevent VMware Identity Manager users from logging in.

Problem

You configure vRealize Automation to access the network through a proxy server, and VMware Identity Manager users see the following error when they attempt to log in.

```
Error Unable to get metadata
```

Solution

Prerequisites

Configure vRealize Automation to access the network through a proxy server. See Connect to the Network Through a Proxy Server.

Procedure

1. Log in to the console of the vRealize Automation appliance as root.
2. Open the following file in a text editor.

   ```
   /etc/sysconfig/proxy
   ```
3. Update the `NO_PROXY` line to ignore the proxy server for VMware Identity Manager logins.

   ```
   NO_PROXY=vrealize-automation-hostname
   ```

   For example: `NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"`
4. Save and close `proxy`.
5. Restart the Horizon workspace service by entering the following command.

   ```
   service horizon-workspace restart
   ```