Installation and Configuration

vRealize Automation 6.2

vmware®

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

vRealize Automation Installation and Configuration

vRealize Automation Installation and Configuration explains how to install and configure 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.

vCloud Suite Licensing and Integration

You can license vRealize Automation individually or as part of vCloud Suite. You should consider the licensing and integration options that are available to you.

Some vCloud Suite components are available as standalone products that are licensed on a per-virtual machine basis. When the products are part of vCloud Suite, they are licensed on a per-CPU basis. You can run an unlimited number of virtual machines on CPUs that are licensed with vCloud Suite. For more information, see *vCloud Suite Architecture Overview and Use Cases*.

VMware Technical Publications Glossary

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

Updated Information

The following table provides update history for the *Installation and Configuration* guide.

Revision	Description
EN-001649-07	■ Revisions for vRealize Automation 6.2.5 including minor updates and bug fixes. ■ Revised Specify Server and Account Settings
EN-001649-06	■ Installation instructions for vRealize Automation 6.2.4 including minor updates and bug fixes.
EN-001649-05	■ Enhanced Distributed Deployment procedures for appliance database configuration.
EN-001649-04	■ Stand-alone PostgreSQL implementations are no longer supported. The PostgreSQL database is now referred to as the appliance database. Changes made to all related topics. ■ For 6.2.2, updated .NET requirement to .NET 4.5.1 or later. ■ Updated IaaS Windows Server requirements to specify Java 1.7 or later. See IaaS Web Service and Model Manager Server Requirements. ■ Added information about the relationship between the user's identity store and the Identity Appliance domain to User Accounts and Credentials Required for Installation and Log in to the vRealize Automation Console Fails. ■ Added a note about using the `iisreset` command before reinstalling IaaS to Roll Back a Minimal Installation and Roll Back a Distributed Installation. ■ Updated Install the Primary IaaS Website Component with Model Manager Data and Failed to Install Model Manager Data and Web Components. ■ Added port 902 to outgoing ports for the vRealize Appliance and moved port 8444 from outgoing ports to incoming ports in Port Requirements. ■ Added additional IaaS service user requirements to User Accounts and Credentials Required for Installation.
EN-001649-03	Added port requirements for VMRC and high-availability deployments in the topic Port Requirements.

EN-001649-02	■ Added `version_string` argument to the topic Create the IaaS Database Manually.
	■ Corrected default location for installation logs in the topic Default Log Locations.
	■ Clarification of steps in the following topics:
	  ■ Update the vRealize Appliance with the Identity Appliance Certificate
	  ■ Update the vRealize Appliance with the IaaS Certificate

Revision	Description
EN-001649-01	■ Updated IaaS Windows Server requirements to specify Java 1.7 and .NET 4.5.1 and later. See IaaS Web Service and Model Manager Server Requirements. ■ Various editorial changes and defect fixes. ■ Revised and updated documentation for Management Agents. See Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate ■ Added step to select Mark this key as exportable when importing a new IIS certificate. See Replace the Internet Information Services Certificate.
EN-001649-00	Initial document release.

vRealize Automation Installation Overview

1

vRealize Automation can be deployed in a variety of configurations. To ensure a successful deployment understand the deployment and configuration options, and the sequence of tasks required.

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

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

This chapter includes the following topics:

vRealize Automation Installation Components

A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

An installation consists of the following components.

- VMware vCloud Automation Center Appliance, which deploys the vCloud Automation Center console (the user interface portal), and manages Single Sign-On (SSO) capabilities for authorization and authentication.
- Infrastructure as a Service (IaaS) components, which are installed on a Windows machine (virtual or physical), and appear largely under the **Infrastructure** tab on the console.
- An SQL Server Database, which can be installed as part of IaaS or separately.
- VMware Identity Appliance

  Identity Appliance is a preconfigured virtual appliance that provides single sign-on (SSO) capabilities for the vRealize Automation environment.
- VMware vRealize Appliance

  The vRealize Appliance is a preconfigured virtual appliance that deploys the vRealize Automation server. vRealize Automation is delivered as an open virtualization format (OVF) template. The system administrator deploys the virtual appliance to an existing virtualized infrastructure.

- vRealize Automation Infrastructure as a Service

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

VMware Identity Appliance

Identity Appliance is a preconfigured virtual appliance that provides single sign-on (SSO) capabilities for the vRealize Automation environment.

You can use the Identity Appliance SSO provided with vRealize Automation or some versions of the SSO provided with vSphere. For information about supported versions, see *vRealize Automation Support Matrix* for this release available from https://www.vmware.com/support/pubs/vcac-pubs.html.

The Identity Appliance is delivered as an open virtualization format (OVF) template. The system administrator deploys the virtual appliance to the existing virtualization infrastructure.

SSO is an authentication broker and security token exchange that interacts with the enterprise identity store, Active Directory or OpenLDAP, to authenticate users. A system administrator configures SSO settings to provide access to the Identity Appliance console.

VMware vRealize Appliance

The vRealize Appliance is a preconfigured virtual appliance that deploys the vRealize Automation server. vRealize Automation is delivered as an open virtualization format (OVF) template. The system administrator deploys the virtual appliance to an existing virtualized infrastructure.

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

Appliance Database

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

vRealize Automation Infrastructure as a Service

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

The system administrator installs IaaS components on a Windows machine, virtual or physical. IaaS capabilities are then available from the **Infrastructure** tab on the user interface console. IaaS has several components that you can install in a custom configuration to meet the needs of your organization.

IaaS Website

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

Model Manager

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

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

vCloud Automation Center Manager Service

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

IaaS Database

The IaaS component of vRealize Automation uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies. Typically, a system administrator creates the database during installation.

Distributed Execution Managers

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

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

The DEM Orchestrator performs these specific tasks.

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

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

vRealize Automation Agents

vRealize Automation uses agents to integrate with external systems. A Management Agent is installed automatically on each IaaS node that you create. You can install the vSphere agent as part of a minimal installation. You can install additional agents as needed by using the Custom Installer.

Integration Agents

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

External provisioning integration (EPI) PowerShell agents allow vRealize Automation to integrate external systems into the machine provisioning process. For example, integration with Citrix Provisioning Server enables provisioning of machines by on-demand disk streaming, and an EPI agent allows you to run Visual Basic scripts as extra steps during the provisioning process.

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

Management Agent

The Management Agent collects support and telemetry information and registers IaaS nodes. A Management Agent is installed automatically on each IaaS node in your deployment.

Management Agents are not automatically deleted when you uninstall an IaaS component. Uninstall the Management Agent as you would uninstall any Windows service.

Virtualization Proxy Agents

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

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

Windows Management Instrumentation Agent

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

Choosing Your Deployment Path

You can upgrade from an earlier vCloud Automation Center 6.x version, migrate from a supported vCloud Automation Center 5.2.x version, or install vRealize Automation for the first time.

Table 1-1. Choosing Your Deployment Path

Your Currently Installed Version	How to install the latest vRealize Automation
vCloud Automation Center 5.2.1	Migrate to vCloud Automation Center 6.1 and then perform upgrades incrementally until you reach the latest version. See *Migrating to vCloud Automation Center 6.1* and *Upgrading to vRealize Automation 6.2 or Later*.
vCloud Automation Center 5.2.2	Migrate to vCloud Automation Center 6.1 and then perform upgrades incrementally until you reach the latest version. See *Migrating to vCloud Automation Center 6.1* and *Upgrading to vRealize Automation 6.2 or Later*.
vCloud Automation Center 5.2.3	Migrating to vRealize Automation
vCloud Automation Center 6.0	Upgrading vRealize Automation
vCloud Automation Center 6.0.1	Upgrading vRealize Automation
vCloud Automation Center 6.1.x	Upgrading vRealize Automation
None	Install vRealize Automation for the first time in either a minimal or distributed deployment. ■ Minimal deployments are typically used in a development environment or as a proof of concept (PoC). You deploy a single instance of each virtual appliance and install all IaaS components on a single Windows machine. You can install the databases on the same Windows machine or on a dedicated SQL Server. See Minimal Deployment Overview. ■ Distributed deployments are typically as a production environment and allow you to design the topology best suited to your organizational needs. You distribute components across multiple servers to provide failover capability and redundancy. See Distributed Deployment Overview. For information about scalability and high availability, see *VMware vRealize Automation Reference Architecture* at https://www.vmware.com/support/pubs/vcac-pubs.html.

Upgrading vRealize Automation

You upgrade incrementally from vRealize Automation 6.x until you reach the latest vRealize Automation.

Locate your currently installed version in the table and then follow the steps in the documents on the right to incrementally upgrade your vRealize Automation environment to the latest release. You can find links to the documentation for all versions of vCloud Automation Center and vRealize Automation at https://www.vmware.com/support/pubs/vcac-pubs.html.

Table 1-2. Supported Upgrade Paths

Your Currently Installed Version	Documentation for Incremental Upgrades
vCloud Automation Center 6.0	Perform upgrades in the following order: ■ *Upgrading vCloud Automation Center 6.0 to 6.0.1* ■ *Upgrading to vCloud Automation Center 6.1* ■ *Upgrading to vRealize Automation 6.2 or Later*
vCloud Automation Center 6.0.1	Perform upgrades in the following order: ■ *Upgrading to vCloud Automation Center 6.1* ■ *Upgrading to vRealize Automation 6.2 or Later*
vCloud Automation Center 6.1.x	*Upgrading to vRealize Automation 6.2 or Later*
vRealize Automation 6.2.x	Upgrade directly to the latest 6.2.x release as described in *Upgrading to vRealize Automation 6.2 or Later*

Migrating to vRealize Automation

You can migrate your data from vCloud Automation Center 5.2.3 to vRealize Automation 6.2.

The following high-level overview shows the steps required to migrate to vRealize Automation 6.2.

1 Read *Migrating vCloud Automation Center 5.2.3 to vRealize Automation 6.2.* for important information about processes and prerequisites.

2 Verify that the Identity Appliance and Windows IaaS servers belong to the same domain as the source vRealize Automation system servers or to a domain with identical domain trusts to the source system servers.

3 Install vRealize Automation 6.2. Depending on your deployment type, see Chapter 4 Minimal Deployment or Chapter 5 Distributed Deployment. As you install, note the following configurations required for migration:

   ■ Join your Identity Appliance to your Native Active Directory domain. See Configure the Identity Appliance.

   ■ Verify that the names of Distributed Execution Orchestrators and Distributed Execution Workers for vRealize Automation 6.2 exactly match the names you used in your vCloud Automation Center 5.2.3 deployment. See Install the Distributed Execution Managers.

   ■ Verify that agent and proxy agent names for vRealize Automation 6.2 exactly match the names you used in your vCloud Automation Center 5.2.3 deployment. See Chapter 6 Installing Agents.

   ■ Configure the default tenant ID store for Native Active Directory. See Configure a Native Active Directory Identity Store.

   ■ You must appoint one or more users to the administrative roles. Groups are not supported for migration. See Appoint Administrators.

4 Migrate your 5.2.3 deployment to vRealize Automation 6.2 using the migration tool. See *Migrating vCloud Automation Center 5.2.3 to vRealize Automation 6.2.*.

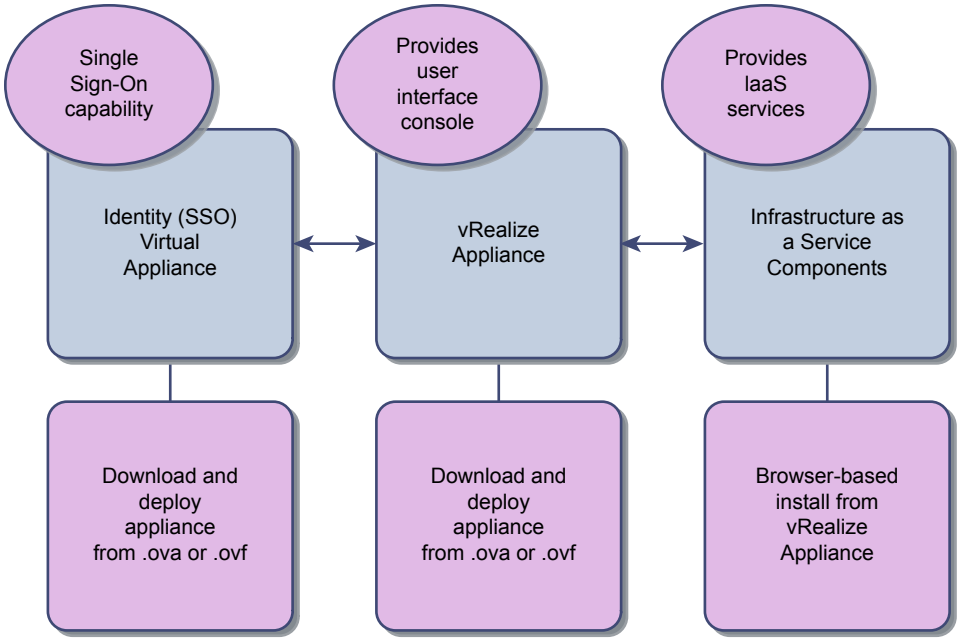
Minimal Deployment Overview

To complete a minimal deployment, the system administrator installs the Identity Appliance, the vRealize Appliance, and Infrastructure as a Service (IaaS).

- Identity Appliance, which supports single sign-on capabilities. It is installed as a virtual appliance.
- vRealize Appliance, which includes the Web console interface. It is installed as a virtual appliance.
- Infrastructure as a Service (IaaS), which is installed on a Windows Server machine.

The IaaS database can be installed on the same machine as IaaS or on its own server.

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



Distributed Deployment Overview

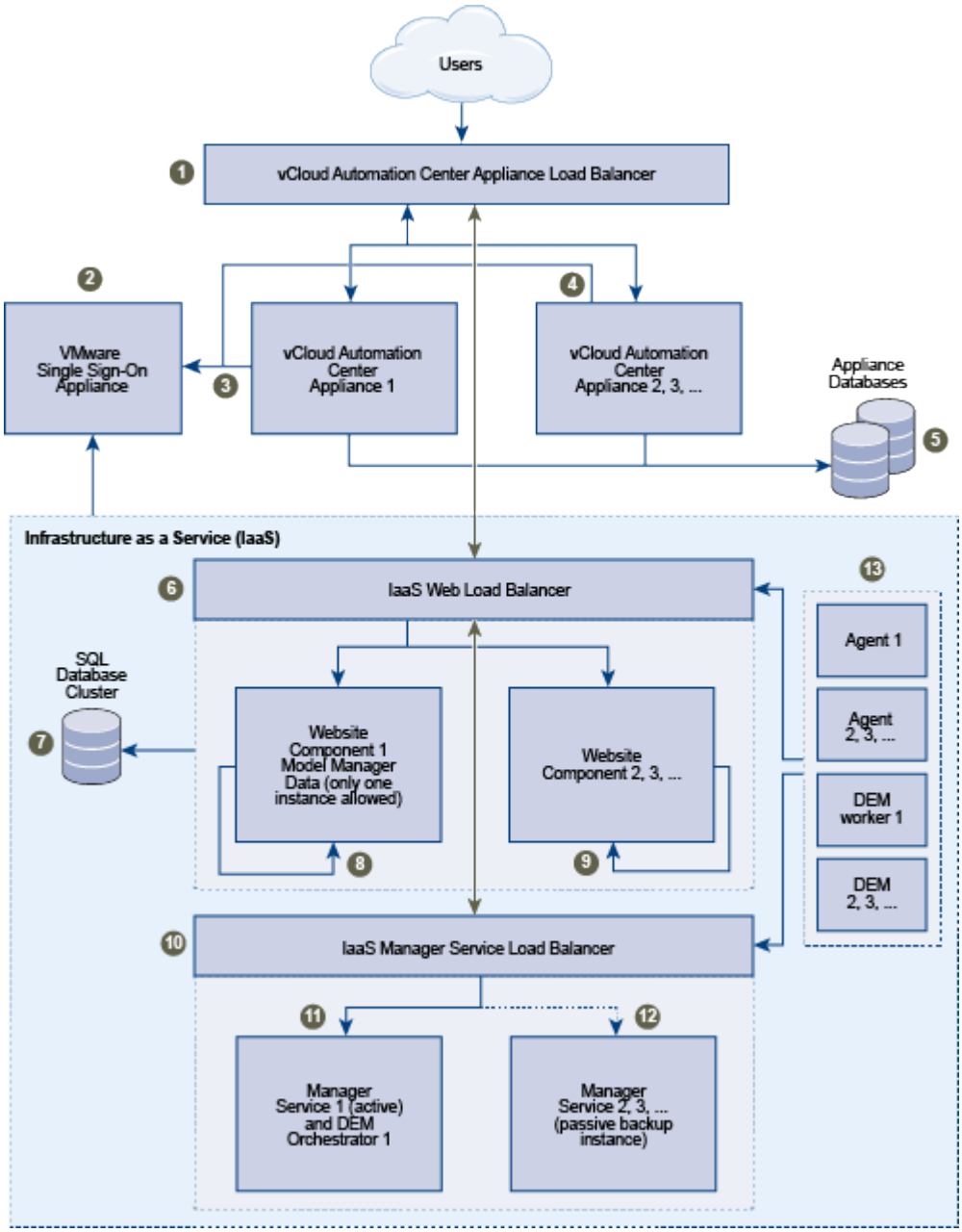
The system administrator can deploy and install multiple instances of the vRealize Appliance and individual IaaS components for scale, redundancy, high availability, and disaster recovery.

In this sample architecture, the IaaS components are distributed over multiple machines. This sample installation describes one possible deployment. Load balancers distribute the workload across the servers. In practice, the system administrator chooses a distribution architecture that is compatible with the company environment and goals.

For information about scalability and high availability, see *VMware vRealize Automation Reference Architecture* at https://www.vmware.com/support/pubs/vcac-pubs.html.

Load balancers distribute the workload across the computing environment. System administrators configure load balancers outside of the vRealize Automation framework.

The following figure shows the components of a distributed deployment. Each component is numbered to correspond to an entry the Distributed Deployment Components table.



The Distributed Deployment Components table describes each component and presents requirements and options for using each component.

Table 1-3. Distributed Deployment Components

Diagram Number	Description	Requirements and Options
1	vRealize Appliance Load Balancer	Only necessary if you are deploying more than one vRealize Appliance. **Important** Disable all nodes under the load balancer except for the node you are configuring. For example, if you have three nodes, disable nodes 1 and 2 when you configure node 3.
2	Single Sign-On Server Appliance	One instance of a single sign-on server is required. You can use the vRealize Appliance, which is a product component, or some versions of vSphere SSO, which might be preferable for high-availability deployments. Consult the *vCloud Automation Center Support Matrix* for information about supported versions.
3	vRealize Appliance 1	One instance required. Multiple instances can be used to support high availability and failover recovery. Multiple instances must be deployed with vSphere High Availability.
4	vRealize Appliance 2, 3, and so on	Deploy multiple instances under the vRealize Appliance Load Balancer.
5	Appliance Database	Appliance Database or cluster. If a two vRealize Appliances have been deployed with Appliance Databases, then they can be clustered. If only one vRealize appliance exists, then there is no highly available method for the database.
6	IaaS Web Load Balancer	Only necessary if you are installing more than one Website Component. Install Website Component 1 and Model Manager Data on one machine under this load balancer.
7	SQL Database Cluster	Install one instance during IaaS installation. Database administrator handles redundancy outside of IaaS context. See Choosing an IaaS Database Scenario.
8	Website Component 1 and Model Manager Data	Required. Install together on one machine under the IaaS Web load balancer. Only one instance of Model Manager Data is allowed. See Install the Primary IaaS Website Component with Model Manager Data
9	Website Component 2, 3, and so on	Optional. Install multiple instances under the IaaS Web load balancer for high availability and failover recovery.
10	IaaS Manager Service Load Balancer	Install the first instance of the Manager Service and the first instance of the DEM Orchestrator together on one machine under this load balancer. See Install the Primary Manager Service and Install the Distributed Execution Managers.
11	Manager Service 1 and DEM Orchestrator 1	Install the first instance of the Manager Service and the first instance of the DEM Orchestrator together on one machine under the IaaS Manager Service load balancer. The first Manager Service instance is active. Only one can be active at any given time. See Install the Primary Manager Service and Install the Distributed Execution Managers.
12	Manager Service 2, 3, and so on	Passive instances for backup only. If the Active Manager Service fails, start the service on the passive node.
13	Agents and DEMs	Install the first DEM Orchestrator on the active Manager Service machine. Install Agents, DEM Orchestrators, and DEM Workers together or on separate machines. See Chapter 6 Installing Agents and Install the Distributed Execution Managers.

Preparing for Installation 2

System Administrators install vRealize Automation into their existing virtualization environments. Before the installation begins, there are a number of preliminary steps that must be completed to prepare the deployment environment.

This chapter includes the following topics:

DNS and Host Name Resolution

vRealize Automation requires the system administrator to identify all hosts using a fully qualified domain name (FQDN). In a distributed deployment, all vRealize Automation components must be able to resolve each other by using an FQDN. The Model Manager Web service, Manager Service, and Microsoft SQL Server database must also be able to resolve each other by their Windows Internet Name Service (WINS) name. You must configure the Domain Name System (DNS) to resolve these host names in your environment.

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

Hardware and Virtual Machine Requirements

Installation requires minimum system resources to install virtual appliances and minimum hardware requirements to install IaaS components on the Windows Server.

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

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

Table 2-1. Hardware Requirements

Identity Appliance	vRealize Appliance	IaaS Components (Windows Server)
1 CPU	2 CPUs	2 CPUs
2 GB memory	8 GB memory	8 GB memory
2 GB disk storage	30 GB disk storage	30 GB disk storage

Browser Considerations

Some restrictions exist for browser use with vRealize Automation.

- vRealize Automation does not support Compatibility View mode for Internet Explorer 9 or 10 on Windows 7 platforms. If you are unable to log in to appliance management consoles or you receive an error on the SSO tab when using Internet Explorer 9 or 10, use the Developer Tools to set the browser mode to Internet Explorer 7.
- Multiple browser windows and tabs are not supported. vRealize Automation supports one session per user.
- VMware remote consoles provisioned on vSphere support a subset of vRealize Automation-supported browsers.

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

Password Considerations

The vRealize Automation administrator password cannot contain a trailing "=" character.

Verify that the adminstrator password you assign during installation does not end with an "=" character. Such passwords are accepted when you assign them, but result in errors when you perform operations such as saving endpoints.

Windows Server Requirements

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

IaaS Database Server Requirements

Your environment must meet these general requirements that support the installation of the IaaS Database (SQL Server).

- TCP/IP protocol enabled for MS SQL Server
- Microsoft Distributed Transaction Coordinator Service (MS DTC) enabled on all SQL nodes in the system. MS DTC is required to support database transactions and actions such as workflow creation.
- No firewalls between Database Server and the Web server or IaaS Server, or ports opened as described in Port Requirements.
- For 6.0.x installations, the database name cannot contain a space. For 6.1 and later installations, the use of spaces in names is supported.

Note If you clone an IaaS node, install MS DTC on each node after it has been cloned. When you clone a node that has MS DTC installed, its unique identifier is copied to each clone, which causes communication to fail. See Error in Manager Service Communication for further information.

For information about supported MS SQL versions, see *vRealize Automation Support Matrix* for this release.

IaaS Web Service and Model Manager Server Requirements

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

IaaS Server Requirements

Your Windows server must meet the configuration requirements listed in the following table to support the installation of the vRealize Automation Web service or Model Manager.

Table 2-2. IaaS Server Requirements

Area	Requirements
Host Configuration	The following components must be installed on the host before installing IaaS: ■ Microsoft .NET Framework 4.5.1 or later ■ Microsoft PowerShell 2.0 (included with Windows Server 2008 R2 SP1 and later) or Microsoft PowerShell 3.0 on Windows Server 2012 or Windows Server 2012 R2. ■ Microsoft Internet Information Services 7.5 (see Table 2-3) ■ Java requirements for MSSQL, when the database is installed on the IaaS Windows server host.

Microsoft SQL Database Requirements	■ Microsoft SQL Server database can be located on the IaaS (Windows) server host or on a remote host.
	■ The following Java-related requirements must be met:
	  ■ A 64-bit version of Java 1.7, or 1.8 or later must be installed. 32-bit versions are not supported.
	  ■ The JAVA_HOME environment variable must be set to the Java installation folder.
	  ■ The %JAVA_HOME%\bin\java.exe file must be available.

Microsoft Internet Information Services Configuration

Microsoft Internet Information Services must be configured to meet the requirements listed in the following table to support the installation of the vRealize Automation Web service or Model Manager.

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

IIS Component	Setting
Internet Information Services (IIS) modules installed	■ WindowsAuthentication ■ StaticContent ■ DefaultDocument ■ ASPNET 4.5 ■ ISAPIExtensions ■ ISAPIFilter
IIS Authentication settings	■ Windows Authentication enabled ■ AnonymousAuthentication disabled ■ Negotiate Provider enabled ■ NTLM Provider enabled ■ Windows Authentication Kernel Mode enabled ■ Windows Authentication Extended Protection disabled ■ For certificates using SHA512, TLS1.2 must be disabled on Windows 2012 or Windows 2012 R2 servers
IIS Windows Process Activation Service roles	■ ConfigurationApi ■ NetEnvironment ■ ProcessModel ■ WcfActivation (Windows 2008 only) ■ HttpActivation ■ NonHttpActivation

IaaS Manager Service

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

- .NET Framework 4.5.1 or later is installed.
- Microsoft PowerShell 2.0 or Microsoft PowerShell 3.0. PowerShell 2.0 is included with Windows Server 2008 R2 SP1 and later. Microsoft PowerShell 3.0 runs on Windows Server 2012 or Windows Server 2012 R2.
- SecondaryLogOnService is running.
- No firewalls can exist between DEM host and Windows Server, nor can ports be opened as described in Port Requirements.
- IIS is installed and configured.

Distributed Execution Manager Requirements

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

- .NET Framework 4.5.1 or later is installed.
- Microsoft PowerShell 2.0 or Microsoft PowerShell 3.0. PowerShell 2.0 is included with Windows Server 2008 R2 SP1 and later. Microsoft PowerShell 3.0 runs on Windows Server 2012 or Windows Server 2012 R2.
- SecondaryLogOnService is running.
- No firewalls between DEM host and the Windows server, or ports opened as described in Port Requirements.

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

Amazon Web Services EC2 Requirements

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

When you use Amazon Web Services for provisioning, DEM workers must meet these configuration requirements.

- Hosts on which DEMs are installed must have access to the Internet.

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

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

Openstack and PowerVC Requirements

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

Table 2-4. DEM Host Requirements

Your Installation	Requirements

All	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`

Windows 2008 DEM Host	In Windows Registry, enable TLS v1.2 protocol. For example:
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]`
	`"DisabledByDefault"=dword:00000000`
	`"Enabled"=dword:00000001`
	
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]`
	`"DisabledByDefault"=dword:00000000`
	`"Enabled"=dword:00000001`

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.

Red Hat Enterprise Virtualization KVM (RHEV) Requirements

Your environment must meet these Red Hat Enterprise requirements to support installation of Distributed Execution Managers (DEMs).

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

SCVMM Requirements

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

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

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

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

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

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

The following additional requirements apply to SCVMM.

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

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

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

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

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

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

- Hyper-V servers within an SCVMM instance to be managed must be Windows 2008 R2 SP1 Servers with Hyper-V installed. The processor must be equipped with the necessary virtualization extensions .NET Framework 4.5.1 or later must be installed and Windows Management Instrumentation (WMI) must be enabled.
- To provision machines on an SCVMM resource, you must add a user in at least one security role within the SCVMM instance.

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

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

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

For more information, see Configure the DEM to Connect to SCVMM at a Different Installation Path. Additional information about preparing for machine provisioning is available in *IaaS Configuration for Virtual Platforms*.

Port Requirements

vRealize Automation uses designated ports for communication and data access.

Although vRealize Automation uses only port 443 for communication, there might be other ports open on the system. Because open, unsecure ports can be sources of security vulnerabilities, review all open ports on your system and ensure that only the ports that are required by your business applications are open.

Identity Appliance

The following ports are used by the Identity Appliance.

Table 2-5. Incoming Ports for the Identity Appliance

Port	Protocol	Comments
22	TCP	Optional. SSH
5480	TCP	Access to virtual appliance Web management interface
7444	TCP	SSO service over HTTPS

Table 2-6. Outgoing Ports for the Identity Appliance

Port	Protocol	Comments
53	TCP, UDP	DNS
67, 68, 546, 547	TCP, UDP	DHCP
80	TCP	Optional. For fetching software updates. Updates can be downloaded separately and applied.
123	TCP, UDP	Optional. For connecting directly to NTP instead of using host time.
389, 636	TCP, UDP	OpenLDAP and Active Directory

vRealize Appliance

The following ports are used by the vRealize Appliance.

Table 2-7. Incoming Ports for the vRealize Appliance

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

Table 2-8. Outgoing Ports for the vRealize Appliance

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

Other ports may be required by specific vRealize Orchestrator plugins that communicate with external systems. For more information, see the documentation for the vRealize Orchestrator plugin.

Infrastructure as a Service

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

Table 2-9. Incoming Ports for Infrastructure as a Service Components

Component	Port	Protocol	Comments
SQL Server instance	1433	TCP	MSSQL
Manager Service	443*	TCP	Communication with IaaS components and vRealize Appliance over HTTPS
vRealize Appliance	443	TCP	Communication with IaaS components and vRealize Appliance over HTTPS

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

Table 2-10. Outgoing Ports for Infrastructure as a Service Components

Component	Port	Protocol	Comments
All	53	TCP, UDP	DNS
All	67, 68, 546, 547	TCP, UDP	DHCP
All	123	TCP, UDP	Optional. NTP.
Manager Service	443	TCP	Communication with vRealize Appliance over HTTPS
Website	443	TCP	Communication with Manager Service over HTTPS
Distributed Execution Managers	443	TCP	Communication with Manager Service over HTTPS
Proxy agents	443	TCP	Communication with Manager Service and virtualization hosts over HTTPS
Guest agent	443	TCP	Communication with Manager Service over HTTPS
Manager Service, Website	1433	TCP	MS SQL

Microsoft Distributed Transaction Coordinator Service

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

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

User Accounts and Credentials Required for Installation

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

vCenter Service Account

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

Virtual Appliance Installation

To deploy the Identity Appliance and the vRealize Appliance, you must have administrator privileges on the deployment platform (for example, vSphere administrator credentials).

During the deployment process, you specify the passwords for the virtual appliance administrator accounts and the system administrator account. These accounts provide access to the Identity Appliance and vRealize Appliance management consoles where you configure and administer the virtual appliances.

IaaS Installation

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

IaaS Database Credentials

You can create the database using the installation wizard or create it manually by running the provided scripts. If you use the **complete** install option to create a minimal installation, you must create the database using the installer.

When you use the IaaS installer to create or populate the IaaS database the following requirements apply:

- If you use the installer to create the database and select **Use Windows Authentication**, the credentials under which you executed the installer must have the **sysadmin** role in SQL Server to create and alter the size of the database.
- If you use the installer to create the database and do not select **Use Windows Authentication**, you must provide SQL credentials with the **sysadmin** role. If you do not use Windows authentication, the credentials you provide are used only for database creation (not for run-time access after initial creation).
- If you use the installer to populate a pre-created database, the user credentials you provide (either the current Windows user or the specified SQL user) needs only **dbo** privileges for the IaaS database.

Note vRealize Automation users also require the correct level of Windows authentication access to log in and use vRealize Automation. The machine from which the user authenticates using Windows Authentication must be joined to the domain in which the vRealize Automation Identity Appliance is configured. See Configure the Identity Stores for the Default Tenant.

IaaS Service User Credentials

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

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

- The user must be a domain user.
- The user must have local Administrator privileges on all hosts on which the Manager Service or Web site component is installed. Do not do a workgroup installation.
- The user is configured with **Log on as a service** privileges. This privilege ensures that the Manager Service starts and generates log files.
- The user must have **dbo** privileges for the IaaS database. If you use the installer to create the database, ensure that the service user login is added to SQL Server prior to running the installer. The installer grants the service user **dbo** privileges after creating the database.
- The account under which the installer is running should have the **sysadmin** role enabled under MSSQL.
- The Management Agent is installed with LocalSystem (NT AUTHORITY\SYSTEM) built-in Windows Account. For more information about Local System accounts, see the Microsoft article http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190%28v=vs.85%29.aspx.
- The domain user account that you plan to use as the IIS application pool identity for the Model Manager Web Service is configured with **Log on as batch job** privileges.

Model Manager Server Specifications

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

Security

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

For more information see Certificate Trust Requirements in a Distributed Deployment and Chapter 9 Updating vRealize Automation Certificates.

Certificates

vRealize Automation uses SSL certificates for secure communication among IaaS components, the Identity Appliance, and instances of the vRealize 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.

If you want to use certificates generated by a certificate authority that is not located on the addressable network, you must modify the web.config file for your web apps to ignore certificate revocation errors. Otherwise, HTTP requests fail with an invalid certificate error.

For important information about troubleshooting, supportability, and trust requirements for certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2106583.

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

Table 2-11. Certificate Implementations

Component	Minimal Deployment (non production)	Distributed Deployment (production ready)
Virtual Appliances	Generate a self-signed certificate during appliance configuration.	For each appliance cluster, obtain a multi-use certificate, such as a Subject Alternative Name (SAN) certificate, from an internal or external certificate authority. Wildcard certificates are also 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. Install the same multi-use certificate on each IaaS installation machine.

Note If you do not have sufficient permissions to install IIS domain certificates, your Web browser prompts you with security exceptions when you open vRealize Automation. Follow the instructions for your browser to permanently trust each self-signed certificate.

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.

Security Passphrase

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

Use the same passphrase for all components in a distributed environment.

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

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

Third-Party Software

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

Time Synchronization

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

Installation fails if time synchronization is set up incorrectly.

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

For virtual machines, you can use the following methods:

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

For Windows servers, consult Timekeeping best practices for Windows, including NTP.

Minimal Deployment Checklist

3

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

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

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

Table 3-1. Minimal Deployment Checklist

	Task	Details
❑	Plan and prepare the installation environment and verify that all installation prerequisites are met.	Chapter 2 Preparing for Installation
❑	Set up your Identity Appliance	Deploy and Configure the Identity Appliance
❑	Set up your vRealize Appliance	Deploy and Configure the vRealize Appliance
❑	Install IaaS components on a single Windows server.	Installing IaaS Components
❑	Install additional agents, if required.	Chapter 6 Installing Agents
❑	Perform post-installation tasks such as configuring the default tenant and entering the IaaS license	Chapter 7 Configuring Initial Access
❑	If needed, configure additional tenants to represent business units in an enterprise or companies that subscribe to cloud services from a service provider.	Chapter 8 Configuring Additional Tenants

Minimal Deployment

4

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.

This chapter includes the following topics:

Minimal Deployment Checklist

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

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

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

Table 4-1. Minimal Deployment Checklist

	Task	Details
❑	Plan and prepare the installation environment and verify that all installation prerequisites are met.	Chapter 2 Preparing for Installation
❑	Set up your Identity Appliance	Deploy and Configure the Identity Appliance
❑	Set up your vRealize Appliance	Deploy and Configure the vRealize Appliance
❑	Install IaaS components on a single Windows server.	Installing IaaS Components
❑	Install additional agents, if required.	Chapter 6 Installing Agents

Table 4-1. Minimal Deployment Checklist (Continued)

	Task	Details
❑	Perform post-installation tasks such as configuring the default tenant and entering the IaaS license	Chapter 7 Configuring Initial Access
❑	If needed, configure additional tenants to represent business units in an enterprise or companies that subscribe to cloud services from a service provider.	Chapter 8 Configuring Additional Tenants

Deploy and Configure the Identity Appliance

Download and configure the Identity Appliance to provide Single Sign-On (SSO) capability for the vRealize Automation environment.

You can use the Identity Appliance SSO provided with vRealize Automation or some versions of the SSO provided with vSphere. For information about supported versions, see *vRealize Automation Support Matrix* for this release available from https://www.vmware.com/support/pubs/vcac-pubs.html.

Note PSC version 6.0, the vSphere SSO component introduced in vSphere 6.0, allows you to specify a tenant name other than vsphere.local. vRealize Automation requires vsphere.local as the name of the default tenant because you cannot enter the name of the tenant on the SSO tab of the management console when you configure vRealize Automation. If you have used another name, rename the tenant to vsphere.local.

1 Deploy the Identity Appliance

   The Identity Appliance is a preconfigured virtual appliance that provides single sign-on capabilities. You download the Identity Appliance and deploy it into vCenter Server or ESX/ESXi inventory.

2 Enable Time Synchronization on the Identity Appliance

   You must synchronize the clocks on the Identity Appliance server, the vRealize Automation server, and Windows servers to ensure a successful installation.

3 Configure the Identity Appliance

   The Identity Appliance provides Single-Sign On (SSO) capability for vRealize Automation users. SSO is an authentication broker and security token exchange that interacts with the enterprise identity store (Active Directory or OpenLDAP) to authenticate users. A system administrator configures SSO settings to provide access to the vRealize Automation.

Deploy the Identity Appliance

The Identity Appliance is a preconfigured virtual appliance that provides single sign-on capabilities. You download the Identity Appliance and deploy it into vCenter Server or ESX/ESXi inventory.

Exact steps for this procedure vary depending on whether you use the native or Web vSphere client. Also, specific steps can vary depending on the your data center configuration. If you are using VSphere Single-Sign (SSO), you can skip to Configure the Identity Appliance.

Prerequisites

- Download the Identity Appliance from the VMware Web site.
- Log in to the vSphere client as a user with **system administrator** privileges.

Procedure

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

   The options that appear depend on your vSphere configuration.
10. Configure the values on the Properties page.
    a. Type the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.
    b. Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

       This value is used to set the initial status of the SSH service in the appliance. You can change this setting from the appliance management console when you configure the appliance.
    c. Type the fully qualified domain name of the virtual machine in the **Hostname** text box, even if you are using DHCP.
    d. Configure the networking properties.
11. Click **Next**.
12. Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.
    - If **Power on after deployment** is available on the Ready to Complete page.
      a. Select **Power on after deployment** and click **Finish**.
      b. Click **Close** after the file finishes deploying into vCenter.

c Wait for the machine to restart. This could take up to five minutes.

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

13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Appliance.

Enable Time Synchronization on the Identity Appliance

You must synchronize the clocks on the Identity Appliance server, the vRealize Automation server, and Windows servers to ensure a successful installation.

If you see certificate warnings during this procedure, continue past them.

Prerequisites

Deploy the Identity Appliance.

Procedure

1 Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.

2 Log in by using the user name root and the password you specified when you deployed the Identity Appliance.

3 Select **Admin > Time Settings**.

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

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

5 Click **Save Settings**.

6 Click **Refresh**.

7 Verify that the value in **Current Time** is correct.

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

Configure the Identity Appliance

The Identity Appliance provides Single-Sign On (SSO) capability for vRealize Automation users. SSO is an authentication broker and security token exchange that interacts with the enterprise identity store (Active Directory or OpenLDAP) to authenticate users. A system administrator configures SSO settings to provide access to the vRealize Automation.

Migration Note If you plan to use the vRealize Automation migration tool, you must specify a Native Active Directory when you configure the appliance.

Native Active Directories have the following characteristics:

- Use Kerberos to authenticate
- Do not require a search base, making it easier to find the correct Active Directory store
- Can be used only with the default tenant

You must also specify an identity store when you configure tenants, even if you specify Native Active Directory settings here.

Prerequisites

Enable Time Synchronization on the Identity Appliance.

Procedure

1. Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.
2. Continue past the certificate warning.
3. Log in with the user name root and the password you specified when the appliance was deployed.

   You can use a service account or user account.
4. Click the **SSO** tab.

   The red text is a prompt, not an error message.
5. Specify a password for the system administrator by entering the same value in the **Admin Password** and **Repeat password** text boxes.

   The **System Domain** text field has the value vsphere.local, which is the local default domain for the Identity Appliance. The default tenant is created with this name and the system administrator is administrator@vsphere.local. Record the user name and password in a secure place for later use.
6. Click **Apply**.

   It can take several minutes for the success message to appear. Do not interrupt the process.
7. When the success message appears, click the **Host Settings** tab.
8. Verify that the **SSO Hostname** does not include a port suffix, such as :7444.

9 (Optional) You can import a certificate or generate a self-signed certificate for the Identity Appliance. A self-signed certificate is also created for you when you deploy the Identity Appliance. Click **SSL**

10 Select the certificate type from the **Choose Action** menu.

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

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Appliance and any load balancer by using Subject Alternative Name (SAN) certificates.

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

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

Option	Action
Import PEM Encoded Certificate	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. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the **Pass Phrase** text box.
Generate Self-Signed Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as *.*mycompany*.com. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

11 Click **Apply Settings**.

After a few minutes the certificate details appear on the page.

12 Join the Identity Appliance to your Native Active Directory domain.

For migration, you must configure Native Active Directory. If you are not using the migration tool, this step is optional.

a Click the **Active Directory** tab.

b Type the domain name of the Active Directory in **Domain Name**.

c Enter the credentials for the domain administrator in the **Domain User** and **Password** text boxes.

d Click **Join AD Domain**.

13 Click the **Admin** tab.

14 Verify that the SSH settings are correct.

When **SSH service enabled** is selected, SSH is enabled for all but the root user. Select or uncheck **Administrator SSH login enabled** to enable or disable SSH login for the root user.

The SSO host is initialized. If your Identity Appliance does not function correctly after configuration, redeploy and reconfigure the appliance. Do not make changes to the existing appliance.

Deploy and Configure the vRealize Appliance

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

1 Deploy the vRealize Appliance

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

2 Enable Time Synchronization on the vRealize Appliance

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

3 Configure the vRealize Appliance

To prepare the vRealize Appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

Deploy the vRealize Appliance

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

Prerequisites

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

Procedure

1 Select **File > Deploy OVF Template** from the vSphere client.

2 Browse to the vRealize Appliance file you downloaded and click **Open**.

3 Click **Next**.

4 Click **Next** on the OVF Template Details page.

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

6 Type a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.

7 Follow the prompts until the Disk Format page appears.

8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.

9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

10 Enter properties for this vRealize Appliance.

a Enter and confirm a password for the vRealize Appliance root account.

This setting can be changed later, from the vRealize Appliance management interface.

b Enable or disable SSH connections to the vRealize Appliance.

This setting can be changed later, from the vRealize Appliance management interface.

c Review the Customer Experience Improvement Program description. If you want to leave the program without joining, you may uncheck the checkbox.

This setting can be changed later, from the vRealize Appliance management interface.

d In the **Hostname** text box, enter the fully qualified domain name of the vRealize Appliance, even if you are using DHCP.

e Enter networking properties.

11 Click **Next**.

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

- If **Power on after deployment** is available on the Ready to Complete page.
  a Select **Power on after deployment** and click **Finish**.
  b Click **Close** after the file finishes deploying into vCenter.
  c Wait for the machine to restart. This could take up to five minutes.
- If **Power on after deployment** is not available on the Ready to Complete page.
  a Click **Close** after the file finishes deploying into vCenter.
  b Power on the VM and wait for some time for the VM to start up.
  c Verify that you can ping the DNS of the VM. If you cannot ping the DNS, restart the VM.
  d Wait for the machine to start. This could take up to five minutes.

13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Appliance.

Enable Time Synchronization on the vRealize Appliance

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

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

Prerequisites

Deploy the vRealize Appliance.

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Log in with the user name root and the password you specified when the appliance was deployed.
3. Select **Admin > Time Settings**.
4. Select an option from the **Time Sync Mode** menu.

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

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

   You can change the time zone as required from the Time Zone Setting page on the **System** tab.
8. (Optional) Click **Time Zone** from the **System** tab and select a system time zone from the menu choices.

   The default is Etc/UTC.
9. Click **Save Settings**.

Configure the vRealize Appliance

To prepare the vRealize Appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

Prerequisites

Enable Time Synchronization on the vRealize Appliance.

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Continue past the certificate warning.
3. Log in with user name root and the password you specified when you deployed vRealize Appliance.
4. Select **vRA Settings > Host Settings**.

Option	Action
Resolve Automatically	Select **Resolve Automatically** to specify the name of the current host for the vRealize Appliance.
Update Host	For new hosts, select **Update Host**. Enter the fully qualified domain name of the vRealize 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 change a host name.

5. Go to the **SSL Configuration** pane.

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

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

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

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

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

Option	Action
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. 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.
Generate Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as *.*mycompany*.com. If you use a load balancer, you need to specify the FQDN of the load balancer or a wildcard that matches the name of the load balancer. If the name is the same as the host name for the virtual appliance, you can leave the text box empty. Do not accept a default value if one is shown, unless it matches the host name of the virtual appliance. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

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

8 Configure the SSO settings.

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

10 Click the **Telemetry** tab.

This product participates in VMware's 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.

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

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

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

12 Configure the license to enable the Infrastructure tab on the vRealize Automation console.

a Click **vRA Settings > Licensing**.

b Click **Licensing**.

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

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

13 Confirm that you can log in to the vRealize Automation console.

a Open a browser and navigate to https://*vcac-hostname.domain.name*/vcac.

b Accept the vRealize Automation certificate.

c Accept the SSO certificate.

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

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

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

What to do next

Install the Infrastructure Components

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 Identity Appliance server, vRealize Automation server, and Windows servers must be synchronized to ensure a successful installation.

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 follows the installation wizard to install the infrastructure components (IaaS) on the Windows virtual or physical machine.

Prerequisites

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

Procedure

1 Download the IaaS Installer

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

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 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 IaaS Installer

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

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

Prerequisites

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

- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. See `res://iesetup.dll/SoftAdmin.htm`.
- Log in to the Windows server as a local administrator.

Procedure

1. Log in to the Windows machine where you are about to perform the installation.
2. Open a Web browser.
3. Enter the URL of the VMware vRealize Automation IaaS Installation download page.

   For example, **`https://vra-va-hostname.domain.name:5480/installer`**, where *vra-va-hostname.domain.name* is the name of the vRealize Appliance host.
4. Download the installer by clicking on the **IaaS Installer** link.
5. When prompted, save the installer file, `setup__vra-va-hostname.domain.name@5480`, to the desktop.

   Do not change the file name. It is used to connect the installation to the vRealize Appliance.

Select the Installation Type

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

Prerequisites

Download the IaaS Installer.

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Appliance. You can view the vRealize 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 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 Under Server Installation Information, enter the user name and password for the Windows service account, which is a local administrator account that also has SQL administrative privileges.

The password for this account cannot contain a double quotation mark (").

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

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

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

3 In the Microsoft SQL Server Database Installation Information panel, accept the default server to install the database instance on the same server with the IaaS components, or type a different server name if the database is on another machine.

   If you specify a different server, you must supply the server name and port number, using the form *servername,portnumber[\NamedInstance]*.

4 Accept the default in the **Database Name** text box or type an appropriate name if applicable.

5 Select the authentication method.

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

6 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 IaaS Installer.

Procedure

1 Accept the default **Server** value, which is populated with the fully qualified domain name of the vRealize 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 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@vsphere.local`** 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 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.

5 Distributed Deployment

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

This chapter includes the following topics:

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 5-1. Distributed Deployment Checklist

Task	Details
❑ Plan and prepare the installation environment and verify that all installation prerequisites are met.	Chapter 2 Preparing for Installation
❑Plan for and obtain your SSL certificates.	Certificate Trust Requirements in a Distributed Deployment
❑ Deploy the Identity Appliance, the lead vRealize Appliance server, and any additional appliances you require for redundancy and high availability.	Deploy Appliances for vRealize Automation

Table 5-1. Distributed Deployment Checklist (Continued)

Task	Details
❑ Configure your load balancer to handle vRealize Automation appliance traffic.	Configuring Your Load Balancer
❑ Configure the Identity Appliance, lead vRealize 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.	Chapter 6 Installing Agents
❑ Configure the default tenant and provide the IaaS license.	Chapter 7 Configuring Initial Access

High-Availability for the Identity Appliance

High-availability and failover protection for the Identity Appliance is handled outside of vRealize Appliance. Use a vSphere HA-enabled cluster to protect the virtual appliance. For more information, see the vSphere documentation center.

vRealize Orchestrator

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

Distributed Installation Components

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

Table 5-2. Virtual Appliances and Appliance Database

Component	Description
Single Sign-On Server	Identity Appliance, a preconfigured virtual appliance that provides Single Sign-On capabilities. Alternatively, you can use some versions of the SSO provided with vSphere. For information on supported versions, see *vRealize Automation Support Matrix*.
vRealize Appliance	A preconfigured virtual appliance that deploys the vRealize Automation server. The server includes the vRealize Automation console, which provides a single portal for self-service provisioning and management of cloud services, as well as authoring and administration.
Appliance Database	Stores information required by the virtual appliances. The database is embedded on one or two vRealize Appliances.

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

Table 5-3. IaaS Components

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

Disabling Load Balancer Health Checks

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

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

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

- When deploying vRealize 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 Appliance and IaaS components, you may re-enable health checks.

Certificate Trust Requirements in a Distributed Deployment

For secure communication, vRealize Appliance relies on certificates to create the trusted relationships between components.

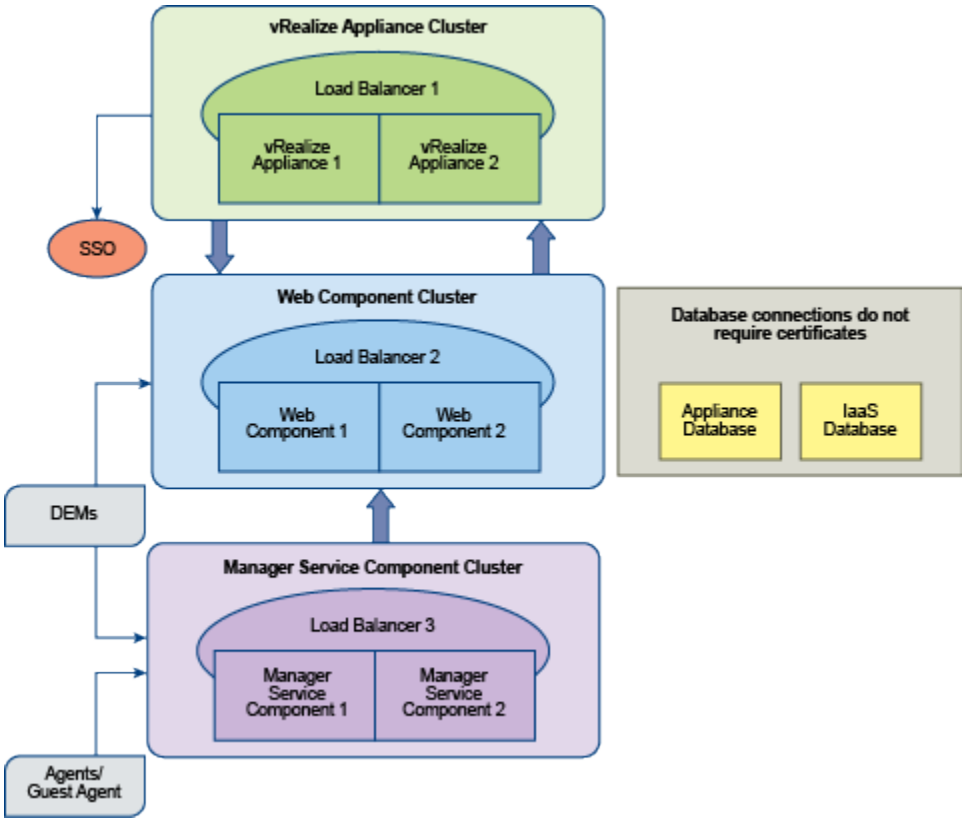
The specific implementation of the certificates required to achieve this trust depends on your environment.

To provide high availability and failover support, you might deploy load balanced clusters of components. In this case, you obtain a multi-use certificate that includes each component in the cluster, and then copy that multi-use certificate to each component in the cluster. You can use Subject Alternative Name (SAN) certificates, chain certificates, wildcard certificates, or any other method of multi-use certification appropriate for your environment as long as you satisfy the trust requirements. Depending on your load balancer configuration, you may need to certify the load balancer as part of the multi-use certificate for the cluster.

For example, if you have a load balancer configuration that requires a certificate on the load balancer as well as its components, you might obtain a SAN certificate to certify web-load-balancer.eng.mycompany.com, web-component-1.eng.mycompany.com, and web-component-2.eng.mycompany.com. You would copy that single multi-use certificate to the load balancer and each of the appliances and then register the certificate on the Web component machines.

The Trust Requirements diagram illustrates the required trust relationships among clusters and assumes you have configured trust as necessary between the load balancer and the nodes underneath it.

Figure 5-1. Trust Requirements



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

Table 5-4. Certificate Importation and Registration

Import	Register
SSO	vRealize Appliance cluster
vRealize Appliance cluster	Web components cluster
Web components cluster	■ vRealize Appliance cluster ■ Manager Service components cluster ■ DEM Orchestrators and DEM Worker components
Manager Service components cluster	■ DEM Orchestrators and DEM Worker components ■ Agents and Proxy Agents

Installation Worksheets

You can use these worksheets to record important information for reference during the installation process.

One copy of each worksheet is given here. Create additional copies as you need them. Settings are case sensitive.

Table 5-5. Identity Appliance Information

Variable	Value	Example
Host Name (FQDN)		vcac-sso.mycompany.com
SSO service over HTTPS Incoming Port	7444 (do not change)	7444
IP		192.168.1.104
Username	administrator@vsphere.local (default)	administrator@vsphere.local
Password		vmware

Table 5-6. Leading cluster vRealize Appliance Information

Variable	Value	Example
Host Name (FQDN)		vcac-va.mycompany.com
SSO service over HTTPS Outgoing Port (default)	7444 (do not change)	7444
IP		192.168.1.105
Username	administrator@vsphere.local (default)	administrator@vsphere.local
Password		vmware

Table 5-7. Additional vRealize Appliance Information

Variable	Value	Example
Host Name (FQDN)		vcac-va2.mycompany.com
SSO service over HTTPS Outgoing Port (default)	7444 (do not change)	7444
IP		192.168.1.110
Username	administrator@vsphere.local (default)	administrator@vsphere.local
Password		vmware

Table 5-8. IaaS Database Passphrase

Variable	Value	Example
Passphrase (reused in IaaS Installer, Upgrade, and Migration)		myPassphrase

Table 5-9. IaaS Website

Variable	Value	Example
Host Name (FQDN)		iaas-web.mycompany.com
SSO service over HTTPS Outgoing Port (default)		
IP		192.168.1.106
Username		
Password		

Table 5-10. IaaS Model Manager Data

Variable	Value	Example
Host Name (FQDN)		iaas-model-man.mycompany.com
SSO service over HTTPS Outgoing Port (default)		
IP		192.168.1.107
Username		
Password		

Table 5-11. IaaS Model Service

Variable	Value	Example
Host Name (FQDN)		iaas-model-service.mycompany.com
SSO service over HTTPS Outgoing Port (default)		
IP		192.168.1.108
Username		
Password		

Table 5-12. Distributed Execution Managers

Unique Name	Orchestrator/Worker
ex. myuniqueorchestratorname	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:

Deploy Appliances for vRealize Automation

Download and deploy all appliances for vRealize Automation.

Procedure

1 Deploy the Identity Appliance

The Identity Appliance is a preconfigured virtual appliance that provides single sign-on capabilities. It is delivered as an open virtualization format (OVF) template. The system administrator downloads the Identity Appliance and deploys it into vCenter Server or ESX/ESXi inventory.

2 Deploy the vRealize Appliance

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

What to do next

If you plan to use a load balancer in your environment, install and configure the load balancer for vRealize Automation traffic. See Configuring Your Load Balancer.

Deploy the Identity Appliance

The Identity Appliance is a preconfigured virtual appliance that provides single sign-on capabilities. It is delivered as an open virtualization format (OVF) template. The system administrator downloads the Identity Appliance and deploys it into vCenter Server or ESX/ESXi inventory.

Prerequisites

- Verify that the Identity Appliance was downloaded from the VMware Web site.
- Log in to the vSphere client as a user with **system administrator** privileges.

Procedure

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

   The options that appear depend on your vSphere configuration.
10. Configure the values on the Properties page.
    a. Type the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.
    b. Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

       This value is used to set the initial status of the SSH service in the appliance. You can change this setting from the appliance management console when you configure the appliance.

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

d Configure the networking properties.

11 Click **Next**.

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

- If **Power on after deployment** is available on the Ready to Complete page.
  a Select **Power on after deployment** and click **Finish**.
  b Click **Close** after the file finishes deploying into vCenter.
  c Wait for the machine to restart. This could take up to five minutes.
- If **Power on after deployment** is not available on the Ready to Complete page.
  a Click **Close** after the file finishes deploying into vCenter.
  b Power on the VM and wait for some time for the VM to start up.
  c Verify that you can ping the DNS of the VM. If you cannot ping the DNS, restart the VM.
  d Wait for the machine to start. This could take up to five minutes.

13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Appliance.

Deploy the vRealize Appliance

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

Prerequisites

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

Procedure

1 Select **File > Deploy OVF Template** from the vSphere client.

2 Browse to the vRealize Appliance file you downloaded and click **Open**.

3 Click **Next**.

4 Click **Next** on the OVF Template Details page.

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

6 Type a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.

7 Follow the prompts until the Disk Format page appears.

8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.

9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

10 Enter properties for this vRealize Appliance.

a Enter and confirm a password for the vRealize Appliance root account.

This setting can be changed later, from the vRealize Appliance management interface.

b Enable or disable SSH connections to the vRealize Appliance.

This setting can be changed later, from the vRealize Appliance management interface.

c Review the Customer Experience Improvement Program description. If you want to leave the program without joining, you may uncheck the checkbox.

This setting can be changed later, from the vRealize Appliance management interface.

d In the **Hostname** text box, enter the fully qualified domain name of the vRealize Appliance, even if you are using DHCP.

e Enter networking properties.

11 Click **Next**.

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

- If **Power on after deployment** is available on the Ready to Complete page.
  a Select **Power on after deployment** and click **Finish**.
  b Click **Close** after the file finishes deploying into vCenter.
  c Wait for the machine to restart. This could take up to five minutes.
- If **Power on after deployment** is not available on the Ready to Complete page.
  a Click **Close** after the file finishes deploying into vCenter.
  b Power on the VM and wait for some time for the VM to start up.
  c Verify that you can ping the DNS of the VM. If you cannot ping the DNS, restart the VM.
  d Wait for the machine to start. This could take up to five minutes.

13 To verify that you successfully deployed the appliance, open a command prompt and ping the fully qualified domain name of the vRealize Appliance.

What to do next

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

Configuring Your Load Balancer

After you deploy the appliances for vRealize Automation, you can set up a load balancer to distribute traffic among multiple instances of the vRealize 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 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 information about scalability and high availability, see *VMware vRealize Automation Reference Architecture* at https://www.vmware.com/support/pubs/vcac-pubs.html.

Configuring Appliances for vRealize Automation

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

Configure the Identity Appliance

Configure the Identity Appliance to provide Single Sign-On (SSO) capability for the vRealize Appliance environment.

You can use the Identity Appliance SSO provided with vRealize Automation or some versions of the SSO provided with vSphere. For information about supported versions, see *vRealize Automation Support Matrix* for this release available from https://www.vmware.com/support/pubs/vcac-pubs.html.

In vRealize Automation 6.2, Active Directory connections are handled by vSphere SSO, and most typical deployments can use Active Directory 2003 or newer. Users should ensure that they are using vSphere SSO 5.5b.

1 Enable Time Synchronization on the Identity Appliance

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

2 Configure the Identity Appliance

The Identity Appliance provides Single-Sign On (SSO) capability for vRealize Automation users. SSO is an authentication broker and security token exchange that interacts with the enterprise identity store (Active Directory or OpenLDAP) to authenticate users. A system administrator configures SSO settings to provide access to the vRealize Appliance.

Enable Time Synchronization on the Identity Appliance

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

If you see certificate warnings during this procedure, continue past them.

Prerequisites

Deploy the Identity Appliance.

Procedure

1 Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.

2 Log in by using the user name **`root`** and the password you specified when you deployed the Identity Appliance.

3 Select **Admin > Time Settings**.

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

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

5 Click **Save Settings**.

6 Verify that the value in **Current Time** is correct.

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

Configure the Identity Appliance

The Identity Appliance provides Single-Sign On (SSO) capability for vRealize Automation users. SSO is an authentication broker and security token exchange that interacts with the enterprise identity store (Active Directory or OpenLDAP) to authenticate users. A system administrator configures SSO settings to provide access to the vRealize Appliance.

Migration Note If you plan to use the vRealize Automation migration tool, you must specify a Native Active Directory when you configure the appliance.

Native Active Directories have the following characteristics:

- Use Kerberos to authenticate
- Do not require a search base, making it easier to find the correct Active Directory store
- Can be used only with the default tenant

You must also specify an identity store when you configure tenants, even if you specify Native Active Directory settings here.

Prerequisites

Enable Time Synchronization on the Identity Appliance.

Procedure

1. Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.
2. Continue past the certificate warning.
3. Log in with the user name root and the password you specified when the appliance was deployed.

   You can use a service account or user account.
4. Click the **SSO** tab.

   The red text is a prompt, not an error message.
5. Specify a password for the system administrator by entering the same value in the **Admin Password** and **Repeat password** text boxes.

   The **System Domain** text field has the value vsphere.local, which is the local default domain for the Identity Appliance. The default tenant is created with this name and the system administrator is administrator@vsphere.local. Record the user name and password in a secure place for later use.
6. Click **Apply**.

   It can take several minutes for the success message to appear. Do not interrupt the process.
7. When the success message appears, click the **Host Settings** tab.
8. Verify that the **SSO Hostname** does not include a port suffix, such as :7444.

9 (Optional) Click **SSL**.

You can import a certificate or generate a self-signed certificate for the Identity Appliance. A self-signed certificate is also created for you when you deploy the Identity Appliance.

10 Select the certificate type from the **Choose Action** menu.

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

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Appliance and any load balancer by using Subject Alternative Name (SAN) certificates.

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

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

Option	Action
Import PEM Encoded Certificate	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. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the **Pass Phrase** text box.
Generate Self-Signed Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as *.*mycompany*.com. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

11 Click **Apply Settings**.

After a few minutes the certificate details appear on the page.

12 Join the Identity Appliance to your Native Active Directory domain.

For migration, you must configure Native Active Directory. If you are not using the migration tool, this step is optional.

a Click the **Active Directory** tab.

b Type the domain name of the Active Directory in **Domain Name**.

c Enter the credentials for the domain administrator in the **Domain User** and **Password** text boxes.

d Click **Join AD Domain**.

13 Click the **Admin** tab.

14 Verify that the SSH settings are correct.

When **SSH service enabled** is selected, SSH is enabled for all but the root user. Select or uncheck **Administrator SSH login enabled** to enable or disable SSH login for the root user.

The SSO host is initialized. If your Identity Appliance does not function correctly after configuration, redeploy and reconfigure the appliance. Do not make changes to the existing appliance.

Configure the Primary vRealize Appliance

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

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

Prerequisites

- Deploy Appliances for vRealize Automation.
- Get a domain certificate for the vRealize Appliance. See Certificates.
- Configure the Identity Appliance.

Procedure

1 Enable Time Synchronization on the vRealize Appliance

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

2 Configure an Appliance Database on the Primary vRealize Automation Appliance

Configure an appliance database on the designated primary vRealize Appliance.

3 Configure the vRealize Appliance

To prepare the vRealize Appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

Enable Time Synchronization on the vRealize Appliance

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

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

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Log in with the user name root and the password you specified when the appliance was deployed.
3. Select **Admin > Time Settings**.
4. Select an option from the **Time Sync Mode** menu.

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

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

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

Configure an Appliance Database on the Primary vRealize Automation Appliance

Configure an appliance database on the designated primary vRealize Appliance.

For related information, see the following content:

- *Add a New Hard Disk to a Virtual Machine in vSphere Web Client* in vSphere product documentation.
- *Gracefully Shutting Down a Windows Guest When the Virtual Machine Powers Off (1744)* in the VMware Knowledge Base.

Prerequisites

- Create DNS entry, for example: dbCluster.domain.local
- IP address allocated for load balancer.
- An installed vRealize Appliance freshly deployed and resolvable through DNS.
- The user configuring the Appliance Database must have Administrator access to vSphere in order to add new disks to the vRealize Appliances.
- Download the 2108923_dbCluster.zip file from the VMware Knowledge Base.

  The link is http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2108923 if you need to paste it into a browser.

Procedure

1. Perform a graceful shutdown of the target appliance using shut down guest in the VMware vCenter Server™.
2. Add a 20 GB disk to the virtual appliance by using the VMware vCenter Server™.
3. Power on the appliance.
4. Verify that SSH is enabled on the virtual appliance.
   a. Log in to the Virtual Appliance Management Interface at https://appliance_IP:5480.
   b. Click the **Admin** tab.
   c. Ensure that the **SSH service enabled** and **Administrator SSH login enabled** check boxes are selected.
   d. Click **Save Settings**.
5. Unzip the 2108923_dbCluster.zip file that you downloaded from the VMware Knowledge Base and copy the 2108923_dbCluster.tar file to the appliance.
6. Extract the configureDisk.sh and pgClusterSetup.sh files using the `tar xvf 2108923_dbCluster.tar` command.

```
# tar xvf 2108923_dbCluster.tar
configureDisk.sh
pgClusterSetup.sh
```

7. Locate the disk you added using the `parted –l` command.

   Note For a fresh vRealize Automation deployment, the disk name should be `/dev/sdd`. The name differs depending on the original version of vRealize Automation deployed.

```
# parted –l
...
Error: /dev/sdd: unrecognized disk label
Sector size (logical/physical): 512B/512B
```

8. Configure the disk using the `./configureDisk.sh` *`disk name`* command.

   For a vRealize Automation deployment, the exact command is `./configureDisk.sh /dev/sdd`.

```
# ./configureDisk.sh /dev/sdd
...
Ownership changed successfully
WAL Archive disk configured successfully
```

9. Run the `pgClusterSetup.sh` script using the following command.

   `/pgClusterSetup.sh [–d] <db_fqdn> [–D] <db_vip> [–w] <db_pass> [–r] <replication_password> [–p] <postgres_password>`

Replace the parameters with the following values as appropriate for your system.

Option	Value
[-d]	Database load balancer FQDN
[-D]	Database virtual IP address. Optional, will create /etc/hosts entry.
[-w]	Sets the database password to the specified entry.
[-r]	Replication password. Optional, will use the database password if not set.
[-p]	Postgres password. Optional, will use database password if not set.

For example, `./pgClusterSetup.sh –d pgCluster.domain.local –w changeMe1! –r changeMe1! –p changeMe1!`

Note Update the password from *ChangeMe!* to one that is appropriate for your system. Also, if you are using a load balancer virtual IP, specify the -D parameter using the IP address of the virtual IP.

```
# ./pgClusterSetup.sh –d dbCluster.domain.local –w changeMe1! –r changeMe1! –p changeMe1!
...
Updating vRealize Automation to utilize database cluster fully qualified domain name
Finished
```

Configure the vRealize Appliance

To prepare the vRealize Appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

Note You must use vsphere.local as the name of the default tenant. If you are using vCenter PSC version 6.0 for SSO, and have given the default tenant a different name, rename the tenant to vsphere.local.

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Continue past the certificate warning.
3. Log in with user name root and the password you specified when you deployed vRealize Appliance.

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

Option	Action
Resolve Automatically	Select **Resolve Automatically** to specify the name of the current host for the vRealize Appliance.
Update Host	For new hosts, select **Update Host**. Enter the fully qualified domain name of the vRealize 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 change a host name.

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

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

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

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

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

Option	Action
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. 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.
Generate Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as *.*mycompany*.com. If you use a load balancer, you need to specify the FQDN of the load balancer or a wildcard that matches the name of the load balancer. If the name is the same as the host name for the virtual appliance, you can leave the text box empty. Do not accept a default value if one is shown, unless it matches the host name of the virtual appliance. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

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 Virtual 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 Configure the license to enable the Infrastructure tab on the vRealize Automation console.

a Click **vRA Settings > Licensing**.

b Click **Licensing**.

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

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

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

12 Click the **Telemetry** tab.

This product participates in VMware's Customer Experience Improvement Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

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

13 Click **Save Settings.**

14 Confirm that you can log into vRealize Automation console.

a Open a browser and navigate to https://*vcac-hostname.domain.name*/vcac/.

If you are using a load balancer, the host name must be the fully qualified domain name of the load balancer.

b If prompted, continue past the certificate warnings.

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

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

Configuring Additional Instances of vRealize Appliance

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

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

Enable Time Synchronization on the vRealize Appliance

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

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

Prerequisites

Configure the Primary vRealize Appliance.

Procedure

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

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

3 Select **Admin > Time Settings**.

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

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

5 Click **Save Settings**.

6 Verify that the value in **Current Time** is correct.

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

Configure Appliance Database on the Secondary vRealize Appliance

Configure an appliance database on the designated secondary vRealize Appliance.

For related information, see the following content:

- *Add a New Hard Disk to a Virtual Machine in vSphere Web Client* in vSphere product documentation
- *Gracefully Shutting Down a Windows Guest When the Virtual Machine Powers Off (1744)* in the VMware Knowledge Base.

Prerequisites

- Create DNS entry, for example: dbCluster.domain.local
- IP address allocated for load balancer.
- An installed vRealize Appliance freshly deployed and resolvable through DNS.
- The user configuring the Appliance Database must have Administrator access to vSphere in order to add new disks to the vRealize Appliances.
- Download the 2108923_dbCluster.zip file from the VMware Knowledge Base.

  The link is http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2108923 if you need to paste it into a browser.

Procedure

1 Perform a graceful shutdown of the target appliance using shut down guest in the VMware vCenter Server™.

2 Add a 20 GB disk to the virtual appliance by using the VMware vCenter Server™.

3 Power on the appliance.

4 Verify that SSH is enabled on the virtual appliance.

  a Log in to the Virtual Appliance Management Interface at https://appliance_IP:5480.

  b Click the **Admin** tab.

  c Ensure that the **SSH service enabled** and **Administrator SSH login enabled** check boxes are selected.

  d Click **Save Settings**.

5 Unzip the 2108923_dbCluster.zip file that you downloaded from the VMware Knowledge Base and copy the 2108923_dbCluster.tar file to the appliance.

6 Extract the configureDisk.sh and pgClusterSetup.sh files using the `tar xvf 2108923_dbCluster.tar` command.

```
# tar xvf 2108923_dbCluster.tar
configureDisk.sh
pgClusterSetup.sh
```

7 Locate the disk you added using the `parted –l` command.

Note For a fresh vRealize Automation deployment, the disk name should be `/dev/sdd`. The name differs depending on the original version of vRealize Automation deployed.

```
# parted –l
...
Error: /dev/sdd: unrecognized disk label
Sector size (logical/physical): 512B/512B
```

8 Configure the disk using the `./configureDisk.sh` *`disk name`* command.

For a vRealize Automation deployment, the exact command is `./configureDisk.sh /dev/sdd`.

```
# ./configureDisk.sh /dev/sdd
...
Ownership changed successfully
WAL Archive disk configured successfully
```

9 Run the `pgClusterSetup.sh` script using the following command.

`/pgClusterSetup.sh [–d] <db_fqdn> [–D] <db_vip> [–w] <db_pass> [–r] <replication_password> [–p] <postgres_password>`

Replace the parameters with the following values as appropriate for your system.

Option	Value
[-d]	Database load balancer FQDN
[-D]	Database virtual IP address. Optional, will create /etc/hosts entry.
[-w]	Sets the database password to the specified entry.
[-r]	Replication password. Optional, will use the database password if not set.
[-p]	Postgres password. Optional, will use database password if not set.

For example, `./pgClusterSetup.sh –d pgCluster.domain.local –w changeMe1! –r changeMe1! –p changeMe1!`

Note Update the password from *ChangeMe!* to one that is appropriate for your system. Also, if you are using a load balancer virtual IP, specify the -D parameter using the IP address of the virtual IP.

```
# ./pgClusterSetup.sh –d dbCluster.domain.local –w changeMe1! –r changeMe1! –p changeMe1!
...
Updating vRealize Automation to utilize database cluster fully qualified domain name
Finished
```

Configure Appliance Database Replication on the Secondary Appliance

Configure the secondary or failover virtual appliance to support appliance database replication.

Set up database replication on the designated secondary appliance so that the appliance database on the primary appliance is replicated on the secondary appliance in the case of failover.

Prerequisites

The appliance database is installed and configured as described in *vRealize Automation Installation and Configuration*.

Procedure

1 Log in to the virtual appliance as root using SSH with the `su – postgres` command.

2 Configure replication as the postgres user using the following command.

`./run_as_replica –h <Primary Appliance> –b –W –U replicate`

Replace the parameters with the following values.

Option	Value
[-h]	Hostname of the master database server. Port 5432 is assumed.
[-b]	Take a base backup from the master. This option destroys the current contents of the data directory.
[-W]	Prompt for the password of the user performing the replication.
[-U]	The user performing the replication. Generally this user is replicate.

For example:

```
# su – postgres
  /opt/vmware/vpostgres/current/share/run_as_replica –h app1.domain.local –b –W –U replicate
```

3 Enter the replicate user password when prompted.

4 Type "yes" after verifying the thumb print of the primary machine when prompted.

5 Enter the postgres user password when prompted.

6 Type "yes" in response to the following message.

"Type yes to enable WAL archiving on primary."

7 Type "yes" in response to the following message.

"WARNING: the base backup operation will replace the current contents of the data directory. Please confirm by typing yes."

What to do next

Validate that the replication was successful. See Validate Appliance Database Replication.

Join a vRealize Appliance to a Cluster

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

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

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

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

Note When you add the first node to a cluster, you might need to reimport or recreate the certificate. Also, you should add nodes to a cluster one at a time and not in parallel.

Prerequisites

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

Procedure

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

2 Continue past any certificate warnings.

3 Log in with user name root and the password you specified when deploying the vRealize Appliance.

4 Select **vRA Settings > Cluster**.

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

You can use the FQDN of the primary vRealize Appliance, or any vRealize 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

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

Prerequisites

Join a vRealize Appliance to a Cluster

Procedure

1 Log in to the vRealize Appliance by using SSH.

2 Stop the embedded vRealize Orchestrator service.

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

3 Log out of the vRealize Appliance.

Validate the Distributed Deployment

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

Procedure

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

2 Confirm that you can log in to the vRealize Automation console by navigating to https://*vcac-hostname.domain.name*/vcac, where *vcac-hostname.domain.name* is the address of the load balancer.

3 After you have verified that the new vRealize Appliance is accessible by using the load balancer, re-enable the other nodes.

Test Appliance Database Failover

Test failover functionality from the primary appliance database machine to the secondary machine.

For this test, the appliance database is failed over, and the replica database on the secondary appliance becomes the master database.

Prerequisites

The appliance database is installed and configured on primary and secondary vRealize Appliances as described in *vRealize Automation Installation and Configuration*.

Procedure

1 Log in to your primary, or master, appliance as root using SSH.

2 Stop the vpostgres service using the `service vpostgres stop` command.

A message similar to the following appears.

```
# service vpostgres stop
Stopping VMware vPostgres: Last login: Mon Apr 27 19:49:26 UTC 2015 on pts/0
ok
```

3 Log in to the secondary appliance as root using SSH.

4 Run the `/opt/vmware/vpostgres/current/share/promote_replica_to_primary` command as the postgres user to promote the replica database to master.

```
su – postgres
/opt/vmware/vpostgres/current/share/promote_replica_to_primary
server promoting
```

Note After running this command, the replica database on the secondary appliance becomes the master. The appliance database on the original primary appliance does not become an actual replica until you run the `run_as_replica` command.

5 Log in to the targeted replica appliance machine as root using SSH.

6 Configure replication using the following command.

`./run_as_replica –h` *`master database appliance`* `–b –W –U replicate`

Replace the parameters with the following values.

Option	Value
[-h]	Host name of the master database server. Port 5432 is assumed.
[-b]	Take a base backup from the master. This option destroys the current contents of the data directory.
[-W]	Prompt for the password of the user performing the replication.
[-U]	The user performing the replication. Generally this user is replicate.

For example:

```
# su – postgres
/opt/vmware/vpostgres/current/share/run_as_replica –h app2.domain.local –b –W –U replicate
```

7 Enter the replicate user password when prompted.

8 Type "yes" after verifying the thumb print of the primary machine when prompted.

9 Enter the postgres user password when prompted.

10 Type "yes" in response to the following message.

"WARNING: the base backup operation will replace the current contents of the data directory. Please confirm by typing yes."

What to do next

Validate that the replication was successful. See Validate Appliance Database Replication.

Test Appliance Database Failback

Test that failback from the secondary appliance database machine to the primary machine functions.

For this test, the appliance database is failed back from the secondary appliance to the original primary appliance.

Prerequisites

The appliance database is installed and configured as described in *vRealize Automation Installation and Configuration*.

Procedure

1 Log in to the replica appliance machine, which currently contains the master appliance database, as root using SSH.

2 Stop the vpostgres service using the `service postgres stop` command.

```
# service postgres stop
Stopping VMware vPostgres: Last login: Mon Apr 27 19:49:26 UTC 2015 on pts/0
ok
```

3 Log in to the primary appliance machine as root using SSH.

4 Promote the replicate database to master as the postgres user with the `/opt/vmware/vpostgre/current/share/promote_replica_to_primary` command.

```
# su – postgres
/opt/vmware/vpostgres/current/share/promote_replica_to_primary
server promoting
```

5 Log in to the replica appliance machine as root using SSH.

6 Configure database replication as the postgres user with a command of the form `./run_as_replica–h` *`Primary Appliance`* `–b –W –U replicate`

```
# su – postgres
/opt/vmware/vpostgres/current/share/run_as_replica –h appl.domain.local
–b –W –U replicate
```

7 Enter the replicate user password when prompted.

8 Enter **`yes`** in response to the following message.

```
Warning: the base
             backup operation will replace the current contents of the data directory.
             Please confirm by typing yes.
```

What to do next

Validate that the replication was successful. See Validate Appliance Database Replication.

Validate Appliance Database Replication

When testing failover or failback of the Appliance Database, validate that the database was replicated correctly.

After configuring the Appliance Database on designated master and replica appliance host machines, test that the database on either machine can function with your system.

Prerequisites

Procedure

1 Log in to the appliance that contains the primary or master database.

2 Run the `ps –ef |grep wal` command to validate that the WAL process is running.

```
# ps –ef |grep wal
postgres  4784  4779  0 21:42 ?        00:00:00 postgres: wal writer
process
postgres 20901  4779  0 22:49 ?        00:00:00 postgres: wal sender process replicate
10.26.36.64(55887) streaming 0/70000B8
```

3 Run the `pg_is_in_recovery` command to validate that the master appliance database is ready for read-write connections.

```
su – postgres
/opt/vmware/vpostgres/current/bin/psql vcac
SELECT pg_is_in_recovery () ;
```

The command returns f for false.

```
vcac=# SELECT pg_is_in_recovery () ;
pg_is_in_recovery
–––––––––––––––––––
f
(1 row)
```

4 Quit psql using the `\q` command.

5 Log in to the secondary appliance with the replica database using SSH.

6 Run the `pg_is_in_recovery` command to validate that the replica database is read only.

```
su – postgres
/opt/vmware/vpostgres/current/bin/psql vcac
SELECT pg_is_in_recovery () ;
```

The command returns t for true.

```
vcac=# SELECT pg_is_in_recovery () ;
pg_is_in_recovery
––––––––––––––––––––––
t
(1 row)
```

7 Quit psql using the `\q` command.

Install the IaaS Components in a Distributed Configuration

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

All components must run under the same service account.

Prerequisites

- Configure the Identity Appliance.
- Configure the Primary vRealize Appliance.
- If your site includes multiple instances of vRealize Appliance, Join a vRealize Appliance to a Cluster.

- Verify that your installation servers meet the requirements described in IaaS Web Service and Model Manager Server Requirements.
- 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 IaaS Installer

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

3 Choosing an IaaS Database Scenario

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

4 Install the Primary IaaS Website Component with 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 Website Components

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

6 Install the Primary Manager Service

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

7 Install an Additional Manager Service Component

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

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

You must disable TLS1.2 for certificates using SHA512 on Windows 2012 machines. For more information about disabling TLS1.2, consult the Microsoft Knowledge Base article at http://support.microsoft.com/kb/245030.

Procedure

1 Obtain a certificate from a trusted certificate authority.

2 Open the Internet Information Services (IIS) Manager.

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

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

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

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

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

5 Click **OK**.

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

7 Verify that the certificate and its chain is trusted.

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

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

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

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

What to do next

Download the IaaS Installer.

Download the IaaS Installer

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

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

Prerequisites

- Configure the Primary vRealize Appliance and, optionally, Join a vRealize Appliance to a Cluster.
- Verify that your installation servers meet the requirements described in IaaS Web Service and Model Manager Server Requirements.
- Verify that you imported a certificate to IIS and that the certificate root or the certificate authority is in the trusted root on the installation machine.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

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

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

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

   c Select **HTTP Activation**.

2 Log in to the Windows machine where you are about to perform the installation.

3 Open a Web browser.

4 Enter the URL of the VMware vRealize Automation IaaS Installation download page.

   For example, **`https://vra-va-hostname.domain.name:5480/installer`**, where *vra-va-hostname.domain.name* is the name of your vRealize Appliance host.

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

6 When prompted, save the installer file, `setup__vra-va-hostname.domain.name@5480.exe`, to the desktop.

   Do not change the file name. It is used to connect the installation to the vRealize Appliance.

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

What to do next

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

Choosing an IaaS Database Scenario

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.

Table 5-13. 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, instead of requiring **sysadmin** privileges.	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.

Database Growth Settings

The vRealize Automation IaaS database must be configured with appropriate growth settings to maintain system performance and integrity. These settings allocate memory for database components and log files to grow as your system runs and processes data. VMware provides default growth settings that are applied automatically when the database is created through the installer or with supplied scripts. If you set up your IaaS database manually, you must configure the appropriate growth settings.

The following table shows the default vRealize Automation IaaS database growth settings.

Table 5-14. Default IaaS Database Growth Settings

	Initial Size	Autogrowth	Maximum Size
Database	1024 MB	By 1024 MB	Unlimited
Log File	512 KB	By 10 %	Limited to 2 TB

You can use Microsoft SQL Management Studio to set or review your database growth settings if needed. While you can increase the growth settings as desired for your system configuration, do not set them lower than the VMware recommendations. Doing so, may affect system performance or cause other problems.

You can also set database growth settings with scripts. The script commands to set the IaaS database to VMware defaults are as follows. In these examples, "dbname" is the name of the database.

```
ALTER DATABASE dbname
MODIFY FILE
(NAME = dbname, MAXSIZE = UNLIMITED, FILEGROWTH = 1024MB)
```

```
ALTER DATABASE dbname
MODIFY FILE
(NAME = dbname_log, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)
```

Create the IaaS Database Manually

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

Prerequisites

- .NET 4.5.1 or later must be installed on the SQL Server host.
- Use Windows Authentication, rather than SQL Authentication, to connect to the database.
- Verify the database installation prerequisites. See IaaS Database Server Requirements.
- Download the IaaS database installer scripts from the vRealize Appliance by navigating to https://*vcac-va-hostname.domain.name*:5480/installer/.

Procedure

1. Navigate to the `Database` subdirectory in the directory where you extracted the installation zip archive.
2. Extract the `DBInstall.zip` archive to a local directory.
3. Log in to the Windows database host with sufficient rights to create and drop databases **sysadmin** privileges in the SQL Server instance.
4. Review the database deployment scripts as needed. In particular, review the settings in the `DBSettings` section of `CreateDatabase.sql` and edit them if necessary.

   The settings in the script are the recommended settings. Only `ALLOW_SNAPSHOT_ISOLATION ON` and `READ_COMMITTED_SNAPSHOT ON` are required.
5. Execute the following command with the arguments described in the table.

   ```
   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 5-15. 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 `vcac`.
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 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 system administrator can install the IaaS schema on an empty database. This installation method provides maximum control over database security.

Prerequisites

- Verify the database installation prerequisites. See IaaS Database Server Requirements.
- Download the IaaS database installer scripts from the vRealize Appliance by navigating to https://*vcac-va-hostname.domain.name*:5480/installer/.

Procedure

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

4 Edit `CreateDatabase.sql` and replace all instances of the variables in the table with the correct values for your environment.

Table 5-16. Database Values

Variable	Value
$(*DBName*)	Name of the database, such as vCAC.
$(*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 `CreateDatabase.sql` and edit them if needed.

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

6 Open SQL Server Management Studio.

7 Click **New Query**.

An SQL Query window opens.

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

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

10 Click **Execute**.

The script runs and creates the database.

What to do next

Install the IaaS Components in a Distributed Configuration.

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 IaaS Installer.

Procedure

1 Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.

2 Click **Next**.

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

4 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

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

5 Click **Next**.

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

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

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

9 Click **Next**.

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

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

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

- Select **Use existing empty database** to create the schema in an existing database.
- Type a new database name or type the default name **vcac** to create a new database.

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

14 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 sys admin rights to the SQL Server instance. The credentials used to access the database at runtime can be configured to use SQL credentials.

15 Click **Next**.

16 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.

17 Click **Install**.

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

19 Click **Finish**.

The database is ready for use.

Install the Primary IaaS Website Component with 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 previously installed other components in this environment, verify that you know the passphrase that was created. See Security Passphrase.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

1 Install the Primary IaaS Website Component

The system administrator installs the Model Manager Website component to provide access to infrastructure capabilities in the vRealize Automation Web console.

2 Configure Model Manager Data

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

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

Install the Primary IaaS Website Component

The system administrator installs the Model Manager Website component to provide access to infrastructure capabilities in the vRealize Automation Web console.

Prerequisites

- Create the IaaS Database Using the Installation Wizard.
- Verify that your environment meets the requirements described in IaaS Web Service and Model Manager Server Requirements.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See Security Passphrase.
- 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__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
3. Click **Next**.
4. Accept the license agreement and click **Next**.
5. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.
   b. Select **Accept Certificate**.
   c. Click **View Certificate**.

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

10 Click **Next**.

11 Select **Website** 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 Website component. You can only install Model Manager Data once.

Prerequisites

Install the Primary IaaS Website Component.

Procedure

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

2 Type the fully qualified domain name of the vRealize Appliance in the **Server** text box.

   IP addresses are not recognized.

   For example, **`vra.mycompany.com`**.

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

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

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

   It might take several minutes to download the certificate.

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

6 Click **Accept Certificate**.

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

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

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

Option	Description
If you are using a load balancer	Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, **`IaaS-load-balancer.eng.mycompany.com`**. IP addresses are not recognized.
With no load balancer	Type the fully qualified domain name of the IaaS Website Server. For example, **`IaaS.eng.mycompany.com`**. IP addresses are not recognized.

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

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

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 Website components or install the Manager Service. See Install Additional IaaS Website Components or Install the Primary Manager Service.

Install Additional IaaS Website Components

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

Prerequisites

- Install the Primary IaaS Website Component with Model Manager Data.
- Verify that your environment meets the requirements described in IaaS Web Service and Model Manager Server Requirements.
- If you previously installed other components in this environment, verify that you know the passphrase that was created. See Security Passphrase.
- 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__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.

3 Click **Next**.

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

5 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

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

6 Click **Next**.

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

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

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

10 Click **Next**.

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

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

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

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

15 Select the certificate for this component.

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

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

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

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

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

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

   This is a less secure option.

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

Option	Description
If you are using a load balancer	Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, `IaaS-load-balancer.eng.mycompany.com`.
With no load balancer	Type the fully qualified domain name of the IaaS Website Server. For example, `IaaS.eng.mycompany.com`.

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

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

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 Primary Manager Service.

Install the Primary Manager Service

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

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See Security Passphrase.
- (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.
- .NET Framework 4.5.1 or later is installed.
- Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.
- Verify that the Web site load balancer is configured and that the timeout value for the load balancer is set to a minimum of 180 seconds.
- Install the Primary IaaS Website Component with 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__vra-va-hostname.domain.name@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 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

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

5 Click **Next**.

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

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

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

9 Click **Next**.

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

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

Option	Description
If you are using a load balancer	Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, `IaaS-load-balancer.eng.mycompany.com`.
With no load balancer	Type the fully qualified domain name of the IaaS Website Server. For example, `IaaS.eng.mycompany.com`.

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

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

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

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

16 Select the certificate for this component.

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

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

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

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

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

18 Click **Next**.

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

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

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

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 primary instance, verify that the vCloud Automation Center Service is running and set it to "Automatic" startup type.

Optionally, you can install an additional instance of the Manager Service component as a passive backup that you can start manually if the primary instance fails. See Install an Additional 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 an Additional Manager Service Component

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

Prerequisites

- If you previously installed other components in this environment, verify that you know the passphrase that was created. See Security Passphrase.
- (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.
- .NET Framework 4.5.1 or later is installed.
- Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.

- Verify that the Website load balancer is configured.
- Install the Primary IaaS Website Component with 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__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.

3 Click **Next**.

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

5 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

  b Select **Accept Certificate**.

  c Click **View Certificate**.

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

6 Click **Next**.

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

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

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

10 Click **Next**.

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

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

Option	Description
If you are using a load balancer	Type the fully qualified domain name of the load balancer for the IaaS Website Server. For example, **`IaaS-load-balancer.eng.mycompany.com`**.
With no load balancer	Type the fully qualified domain name of the IaaS Website Server. For example, **`IaaS.eng.mycompany.com`**.

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

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

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

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

17 Select the certificate for this component.

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

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

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

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

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

19 Click **Next**.

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

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

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

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 Distributed Execution Manager Requirements.

Install the Distributed Execution Managers

A system administrator installs at least one DEM Worker and one DEM Orchestrator. The installation procedure is the same for both roles.

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

Prerequisites

Download the IaaS Installer.

Procedure

1 Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.

2 Click **Next**.

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

4 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

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

5 Click **Next**.

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

7 Select **Distributed Execution Managers** under Component Selection on the Installation Type page.

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

9 Click **Next**.

10 Check prerequisites and click **Next**.

11 Enter the log in credentials under which the service will run. This must be a local administrator account.

12 Click **Next**.

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

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

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

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

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

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

Option	Description
If you are using a load balancer	Type the fully qualified domain names of the load balancers for the Manager Service and Model Manager Web Service. For example, `manager-load-balancer.eng.mycompany.com:443` and `web-load-balancer.eng.mycompany.com:443`.
With no load balancer	Type the fully qualified domain names of the Manager Service and Model Manager Web Service. For example, `manager-service.eng.mycompany.com:443` and `model-manager.eng.mycompany.com:443`.

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) 2012 console. You must update the configuration when the SCVMM console is installed to another location.

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

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

Prerequisites

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

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

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

Procedure

1 Stop the DEM Worker service.

2 Open the following file in a text editor.

`Program Files (x86)\VMware\vCAC\Distributed Execution Manager\`*`instance-name`*`\DynamicOps.DEM.exe.config`

3 Locate the `<assemblyLoadConfiguration>` section.

4 Update each `path`, using the following example as a guideline.

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

5 Save and close `DynamicOps.DEM.exe.config`.

6 Restart the DEM Worker service.

For more information, see SCVMM Requirements. Additional information about preparing the SCVMM environment and creating an SCVMM endpoint is available in *IaaS Configuration for Virtual Platforms*.

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.

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.

What to do next

Provide the Infrastructure License.

Installing Agents

6

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.

This chapter includes the following topics:

- Installing the WMI Agent for Remote WMI Requests

Set the PowerShell Execution Policy to RemoteSigned

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

Prerequisites

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

Procedure

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

Choosing the Agent Installation Scenario

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

Table 6-1. 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

Table 6-1. Choosing an Agent Scenario (Continued)

Integration Scenario	Agent Requirements and Procedures
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 6-2. Permissions Required for vSphere Agent to Manage vCenter Server Instance

Attribute Value	Permission
Datastore	Allocate Space
	Browse Datastore
Folder	Create Folder

Table 6-2. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

Attribute Value		Permission
		Delete Folder
Global		Manage Custom Attributes
		Set Custom Attribute
Network		Assign Network
Permissions		Modify Permission
Resource		Assign VM to Res Pool
		Migrate Powered Off Virtual Machine
		Migrate Powered On Virtual Machine
Virtual Machine	Inventory	Create from existing
		Create New
		Migrate Powered On Virtual Machine
		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
		Remove Disk
		Advanced
		Change CPU Count
		Change Resource
		Device Extend Virtual Disk Settings
		Disk Change Tracking
		Memory
		Modify Device Settings
		Rename

Table 6-2. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

Attribute Value		Permission
		Set Annotation (version 5.0 and later)
		Settings
		Swapfile Placement
	Provisioning	Customize
		Clone Template
		Clone Virtual Machine
		Deploy Template
		Read Customization Specs
	State	Create Snapshot
		Remove Snapshot
		Revert to Snapshot

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

Install the vSphere Agent

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

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have completed all the vSphere Agent Requirements.
- If you already created a vSphere endpoint for use with this agent, make a note of the endpoint name.
- Download the IaaS Installer.

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.

4 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

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

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

6 Select **Component Selection** on the Installation Type page.

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

8 Click **Next**.

9 Log in with **administrator** privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.

10 Click **Next**.

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

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

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

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this agent.

13 Configure a connection to the Manager Service component.

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

The default port is 443.

14 Configure a connection to the Manager Website component.

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

The default port is 443.

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

16 Enter the name of the endpoint.

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

17 Click **Add**.

18 Click **Next**.

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

After several minutes a success message appears.

20 Click **Next**.

21 Click **Finish**.

22 Verify that the installation is successful.

23 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

What to do next

Configure the vSphere Agent.

Configure the vSphere Agent

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

Prerequisites

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

Procedure

1 Open a Windows command console as an administrator.

2 Go to the agents installation directory.

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

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

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

```
managementEndpointName: VCendpoint
doDeletes: True
```

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

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

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

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

For example, `Dynamic0ps.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 Navigate to **Start > Administrative Tools > Services** and restart the vRealize Automation Agent – *agentname* service.

What to do next

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

Installing the Proxy Agent for Hyper-V or XenServer

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

Hyper-V and XenServer Requirements

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

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

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

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

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

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

Install the Hyper-V or XenServer Agent

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

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Download the IaaS Installer.
- Verify that Hyper-V Hypervisor proxy agents have system administrator credentials.
- Verify that the credentials under which to run the agent service have administrative access to the installation host.
- Verify that all XenServer or Hyper-V instances on the hosts to be managed by the agent have administrator-level credentials.
- If you are using Xen pools, note that all nodes within the Xen pool must be identified by their fully qualified domain names.

  vRealize Automation cannot communicate with or manage any node that is not identified by its fully qualified domain name within the Xen pool.

- Configure Hyper-V for remote management to enable Hyper-V server communication with vRealize Automation Hyper-V proxy agents.

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

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Appliance. You can view the vRealize Appliance certificate in the client browser when the management console is accessed on port 5480.
5. Select **Custom Install** on the Installation Type page.
6. Select **Component Selection** on the Installation Type page.
7. Accept the root install location or click **Change** and select an installation path.
8. Click **Next**.
9. Log in with **administrator** privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.
11. Select the agent from the **Agent type** list.
    - Xen
    - Hyper-V

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

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

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this 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 Manager Service component.

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

The default port is 443.

15 Configure a connection to the Manager Website component.

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

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.

```
Dynamic0ps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith

Dynamic0ps.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

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that your environment meets the XenDesktop Requirements.
- Download the IaaS Installer.

Procedure

1 Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.

2 Click **Next**.

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

4 On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b Select **Accept Certificate**.

   c Click **View Certificate**.

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

5 Click **Next**.

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

7 Select **Proxy Agents** in the Component Selection pane.

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

9 Click **Next**.

10 Log in with **administrator** privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.

11 Click **Next**.

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this agent.

14 Configure a connection to the Manager Service component.

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

The default port is 443.

15 Configure a connection to the Manager Website component.

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

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

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the Citrix Provisioning Server Requirements.
- Download the IaaS Installer.

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Appliance. You can view the vRealize Appliance certificate in the client browser when the management console is accessed on port 5480.
5. Select **Custom Install** on the Installation Type page.
6. Select **Component Selection** on the Installation Type page.
7. Accept the root install location or click **Change** and select an installation path.
8. Click **Next**.
9. Log in with **administrator** privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.

11 Select **EPIPowerShell** from the Agent type list.

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

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

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this agent.

13 Configure a connection to the Manager Service component.

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

The default port is 443.

14 Configure a connection to the Manager Website component.

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

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 6-3. 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

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the Visual Basic Scripting Requirements.
- Download the IaaS Installer.

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

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

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

6 Select **Component Selection** on the Installation Type page.

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

8 Click **Next**.

9 Log in with **administrator** privileges for the Windows services on the installation machine.

The service must run on the same installation machine.

10 Click **Next**.

11 Select **EPIPowerShell** from the Agent type list.

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

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

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this agent.

13 Configure a connection to the Manager Service component.

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

The default port is 443.

14 Configure a connection to the Manager Website component.

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

The default port is 443.

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

16 Select the EPI type.

17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.

18 Click **Add**.

19 Click **Next**.

20 Click **Install** to begin the installation.

After several minutes a success message appears.

21 Click **Next**.

22 Click **Finish**.

23 Verify that the installation is successful.

24 (Optional) Add multiple agents with different configurations and an endpoint on the same system.

Installing the WMI Agent for Remote WMI Requests

A system administrator enables the Windows Management Instrumentation (WMI) protocol and installs the WMI agent on all managed Windows machines to enable management of data and operations. The agent is required to collect data from Windows machines, such as the Active Directory status of the owner of a machine.

Enable Remote WMI Requests on Windows Machines

To use WMI agents, remote WMI requests must be enabled on the managed Windows servers.

Procedure

1 In each domain that contains provisioned and managed Windows virtual machines, create an Active Directory group and add to it the service credentials of the WMI agents that execute remote WMI requests on the provisioned machines.

2 Enable remote WMI requests for the Active Directory groups containing the agent credentials on each Windows machine provisioned.

Install the WMI Agent

The Windows Management Instrumentation (WMI) agent enables data collection from Windows managed machines.

Prerequisites

- The IaaS components, including the Manager Service and Website, are installed.
- Verify that you have satisfied all the requirements, see Enable Remote WMI Requests on Windows Machines.

- Download the IaaS Installer.

Procedure

1. Right-click the `setup__vra-va-hostname.domain.name@5480.exe` setup file and select **Run as administrator**.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. On the Log in page, supply administrator credentials for the vRealize 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 Appliance.

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

      Compare the certificate thumbprint with the thumbprint set for the vRealize Appliance. You can view the vRealize Appliance certificate in the client browser when the management console is accessed on port 5480.
5. Select **Custom Install** on the Installation Type page.
6. Select **Component Selection** on the Installation Type page.
7. Accept the root install location or click **Change** and select an installation path.
8. Click **Next**.
9. Log in with **administrator** privileges for the Windows services on the installation machine.

   The service must run on the same installation machine.
10. Click **Next**.
11. Select **WMI** from the **Agent type** list.
12. Enter an identifier for this agent in the **Agent name** text box.

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

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

Option	Description
Redundant agent install	Install redundant agents on different servers, but name and configure them identically to provide high-availability.
Single agent install	Select a unique name for this agent.

13 Configure a connection to the Manager Service component.

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

The default port is 443.

14 Configure a connection to the Manager Website component.

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

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.

Configuring Initial Access 7

Before your team can begin setting up for provisioning, you must configure their access to the default tenant by adding an identity store and appointing administrators. If you installed IaaS, you must also provide the infrastructure license.

This chapter includes the following topics:

Configure the Identity Stores for the Default Tenant

Each tenant requires at least one identity store. Identity stores can be OpenLDAP or Active Directory. Active Directory in native mode is supported for the default tenant only.

The default tenant is automatically created when you configure single sign-on. You cannot edit any of the tenant details.

Configure a Native Active Directory Identity Store

You can configure the default tenant identity store for Native Active Directory if you joined the Identity Appliance to your Active Directory domain.

You can configure an Active Directory in native mode for the default tenant only.

Migration Note For migration, you must configure your identity store to use Native Active Directory. Migration is supported only to the default tenant, vsphere.local, in the target system and only if the default tenant is configured for Native Active Directory.

Prerequisites

Verify that your Identity Appliance is joined to your Native Active Directory domain. See Configure the Identity Appliance.

Procedure

1 Log in to the vRealize Automation console as the system administrator of the default tenant.

   a Navigate to the vRealize Automation console.

Option	Description
If you are using a load balancer	https://*vrealize-appliance-load-balancer-hostname.domain.name*/vcac
With no load balancer	https://*vrealize-appliance-hostname.domain.name*/vcac

   b Log in with the user name **`administrator@vsphere.local`** 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 **Identity Stores** tab.

5 Click the **Add** icon ( ).

6 Select **Native Active Directory** from the **Type** drop-down menu.

7 Enter the domain for the identity store in the **Domain** text box.

8 Click **Add**.

9 Click **Update**.

Your new identity store is saved and associated with the tenant. You are directed to the **Administrators** tab for the next step in the process.

What to do next

Appoint Administrators.

Configure an OpenLDAP or Active Directory Identity Store

You can configure identity stores for OpenLDAP or Active Directory in mixed mode without joining your Active Directory domain to the Identity Appliance.

Prerequisites

Install vRealize Automation 6.1, including IaaS components. Depending on your deployment type, see Chapter 4 Minimal Deployment or Chapter 5 Distributed Deployment.

Procedure

1 Log in to the vRealize Automation console as the system administrator of the default tenant.

   a Navigate to the vRealize Automation console.

Option	Description
If you are using a load balancer	https://*vrealize-appliance-load-balancer-hostname.domain.name*/vcac
With no load balancer	https://*vrealize-appliance-hostname.domain.name*/vcac

   b Log in with the user name **`administrator@vsphere.local`** 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 **Identity Stores** tab.

5 Click the **Add** icon ().

6 Enter a name in the **Name** text box.

7 Select **OpenLDAP** or **Active Directory** from the **Type** drop-down menu.

8 Enter the URL for the identity store in the **URL** text box.

   For example, **`ldap://ldap.mycompany.com:389`** .

9 Enter the domain for the identity store in the **Domain** text box.

10 (Optional) Enter the domain alias in the **Domain Alias** text box.

   The alias allows users to log in by using *userid@domain-alias* rather than *userid@identity-store-domain* as a user name.

11 Enter the Distinguished Name for the login user in the **Login User DN** text box.

   Use the display format of the user name, which can include spaces and is not required to be identical to the user ID.

   For example, **`cn=Demo Admin,ou=demo,dc=dev,dc=mycompany,dc=com`**.

12 Enter the password for the identity store login user in the **Password** text box.

13 Enter the group search base Distinguished Name in the **Group Search Base DN** text box.

   For example, **`ou=demo,dc=dev,dc=mycompany,dc=com`**.

14 (Optional) Enter the user search base Distinguished Name in the **User Search Base DN** text box.

   For example, **`ou=demo,dc=dev,dc=mycompany,dc=com`**.

15 Click **Test Connection**.

16 Click **Add**.

17 (Optional) Repeat this procedure to configure additional identity stores.

18 Click **Next**.

19 Click **Update**.

What to do next

Appoint Administrators.

Appoint Administrators

You can appoint one or more tenant administrators and IaaS administrators from the identity stores you configured for a tenant.

Tenant administrators are responsible for configuring tenant-specific branding, as well as managing identity stores, users, groups, entitlements, and shared blueprints within the context of their tenant. IaaS Administrators are responsible for configuring infrastructure source endpoints in IaaS, appointing fabric administrators, and monitoring IaaS logs.

Migration Note For migration, you must select one or more single users to appoint as your administrators. The individual administrator name must have access to the default tenant, vsphere.local. Group administrator names are not supported.

Prerequisites

- Log in to the vRealize Automation console as a **system administrator**.
- Configure the Identity Stores for the Default Tenant.

Procedure

1 Select **Administration > Tenants**.

2 Click the name of the default tenant, **vsphere.local**.

3 Click the **Administrators** tab.

4 Enter the name of a user or group in the **Tenant Administrators** search box and press Enter.

For faster results, enter the entire user or group name, for example myAdmins@mycompany.domain. Repeat this step to appoint additional tenant administrators.

5 If you have installed IaaS, enter the name of a user or group in the **Infrastructure Administrators** search box and press Enter.

For faster results, enter the entire user or group name, for example IaaSAdmins@mycompany.domain. Repeat this step to appoint additional infrastructure administrators.

6 Verify that the user or group names you chose appear in **Tenant Administrators** and **Infrastructure Administrators** lists.

7 Click **Update**.

For migration, make note of the tenant administrator you appointed. You must supply the tenant administrator credentials to the pre-migration tool when you are prompted for the default tenant administrator credentials.

What to do next

Provide the Infrastructure License.

Provide the Infrastructure License

After installation, the IaaS administrator logs into the vRealize Automation console and provides a license for the Infrastructure components.

Prerequisites

Appoint Administrators.

Procedure

1. Navigate to the vRealize Appliance console by using its fully qualified domain name, https://*vra-hostname.domain.name*/vcac/.
2. If you are prompted, accept the certificate.
3. Log in to the vRealize Automation console as a user with the **IaaS administrator** role.

   For example, IaaSAdmin@mycompany.com

   If you are already logged in to the console, log out and log in again.
4. Click the **Infrastructure** tab.
5. Navigate to **Administration > Licensing**.
6. Click **Add License**.
7. Enter the VMware license code in the **License key** text box.
8. Verify that your license key displays in the License Information table.
9. Click **OK**.

What to do next

Repeat this procedure to add additional license keys.

Configuring Additional Tenants

8

You create the default tenant when you install vRealize Automation, but you can create additional tenants to represent business units in an enterprise or companies that subscribe to cloud services from a service provider.

This chapter includes the following topics:

Tenancy Overview

A tenant is an organizational unit in a vRealize Automation deployment. A tenant can represent a business unit in an enterprise or a company that subscribes to cloud services from a service provider.

Each tenant has its own dedicated configuration. Some system-level configuration is shared across tenants.

Table 8-1. Tenant Configuration

Configuration Area	Description
Login URL	Each tenant has a unique URL to the vRealize Automation console. ■ The default tenant URL is in the following format: https://*hostname*/vcac ■ The URL for additional tenants is in the following format: https://*hostname*/vcac/org/*tenantURL*
Identity stores	Each tenant requires access to one or more directory services, such as OpenLDAP or Microsoft Active Directory servers, that are configured to authenticate users. You can use the same directory service for more than one tenant, but you must configure it separately for each tenant.
Branding	A tenant administrator can configure the branding of the vRealize Automation console including the logo, background color, and information in the header and footer. System administrators control the default branding for all tenants.
Notification providers	System administrators can configure global email servers that process email notifications. Tenant administrators can override the system default servers, or add their own servers if no global servers are specified.
Business policies	Administrators in each tenant can configure business policies such as approval workflows and entitlements. Business policies are always specific to a tenant.

Table 8-1. Tenant Configuration (Continued)

Configuration Area	Description
Service catalog offerings	Service architects can create and publish catalog items to the service catalog and assign them to service categories. Services and catalog items are always specific to a tenant.
Infrastructure resources	The underlying infrastructure fabric resources, for example, vCenter servers, Amazon AWS accounts, or Cisco UCS pools, are shared among all tenants. For each infrastructure source that vRealize Automation manages, a portion of its compute resources can be reserved for users in a specific tenant to use.

About the Default Tenant

When the system administrator configures single sign-on during the installation of vRealize Automation, a default tenant is created with the built-in system administrator account to log in to the vRealize Automation console. The system administrator can then configure the default tenant and create additional tenants.

The default tenant supports all of the functions described in Tenant Configuration. In the default tenant, the system administrator can also manage system-wide configuration, including global system defaults for branding and notifications, and monitor system logs.

The default tenant is the only tenant that supports native Active Directory authentication. All other tenants must use Active Directory over OpenLDAP.

User and Group Management

All user authentication is handled through single sign-on. Each tenant has one or more identity stores, such as Active Directory servers, that provide authentication.

The system administrator performs the initial configuration of single sign-on and basic tenant setup, including designating at least one identity store and a tenant administrator for each tenant. Thereafter, a tenant administrator can configure additional identity stores and assign roles to users or groups from the identity stores.

Tenant administrators can also create custom groups within their own tenant and add users and groups defined in the identity store to custom groups. Custom groups, like identity store groups and users, can be assigned roles or designated as the approvers in an approval policy.

Tenant administrators can also create business groups within their tenant. A business group is a set of users, often corresponding to a line of business, department or other organizational unit, that can be associated with a set of catalog services and infrastructure resources. Users, identity store groups, and custom groups can be added to business groups.

Comparison of Single-Tenant and Multitenant Deployments

vRealize Automation supports deployments with either a single tenant or multiple tenants. The configuration can vary depending on how many tenants are in your deployment.

System-wide configuration is always performed in the default tenant and can apply to one or more tenants. For example, system-wide configuration might specify defaults for branding and notification providers.

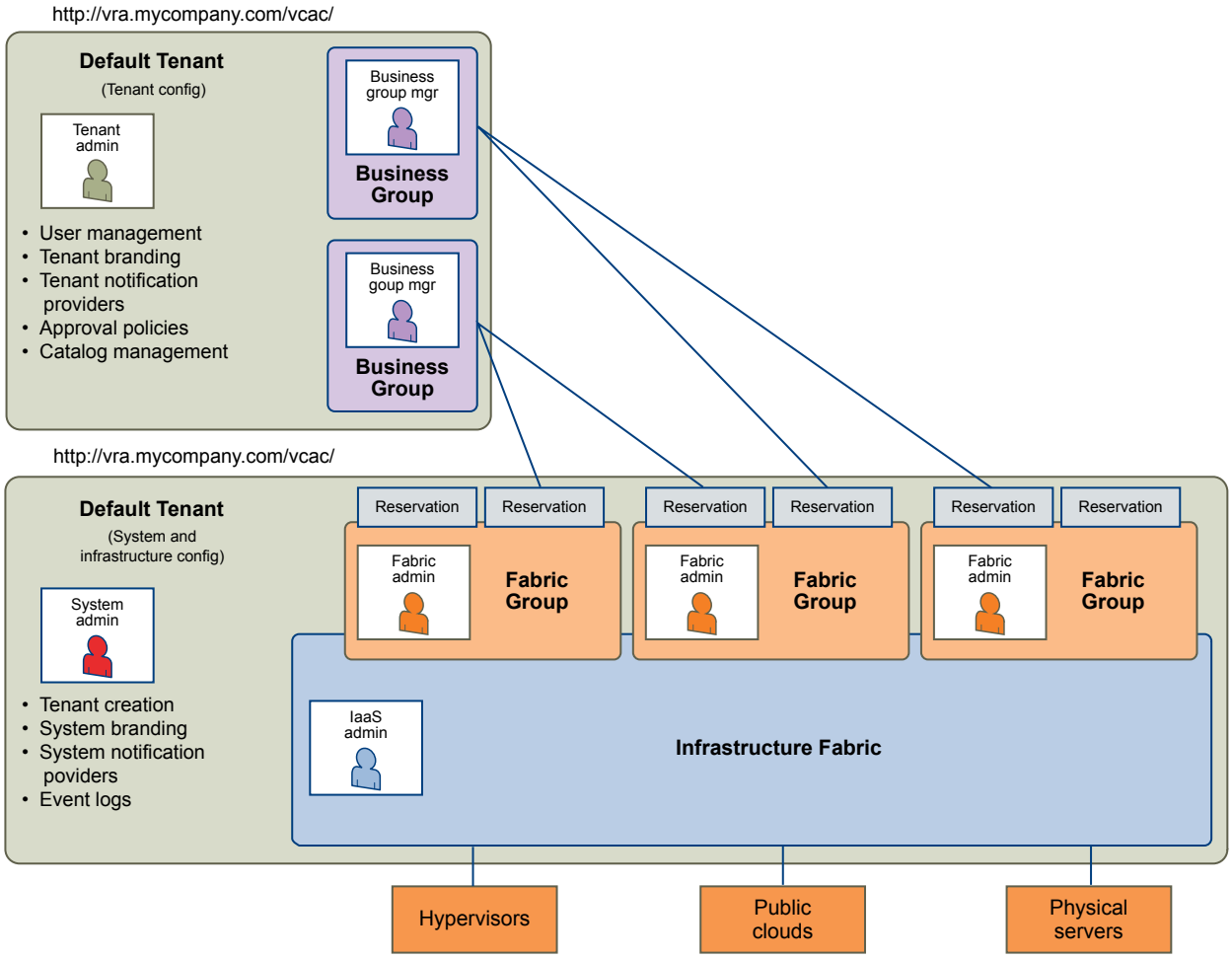
Infrastructure configuration, including the infrastructure sources that are available for provisioning, can be configured in any tenant and is shared among all tenants. The infrastructure resources, such as cloud or virtual compute resources or physical machines, can be divided into fabric groups managed by fabric administrators. The resources in each fabric group can be allocated to business groups in each tenant by using reservations.

Single-Tenant Deployment

In a single-tenant deployment, all configuration can occur in the default tenant. Tenant administrators can manage users and groups, configure tenant-specific branding, notifications, business policies, and catalog offerings.

All users log in to the vRealize Automation console at the same URL, but the features available to them are determined by their roles.

Figure 8-1. Single-Tenant Example



Note In a single-tenant scenario, it is common for the system administrator and tenant administrator roles to be assigned to the same person, but two distinct accounts exist. The system administrator account is always administrator@vsphere.local. The tenant administrator must be a user in one of the tenant identity stores, such as *username*@mycompany.com.

Multitenant Deployment

In a multitenant environment, the system administrator creates tenants for each organization that uses the same vRealize Automation instance. Tenant users log in to the vRealize Automation console at a URL specific to their tenant. Tenant-level configuration is segregated from other tenants and from the default tenant. Users with system-wide roles can view and manage configuration across multiple tenants.

There are two main scenarios for configuring a multi-tenant deployment.

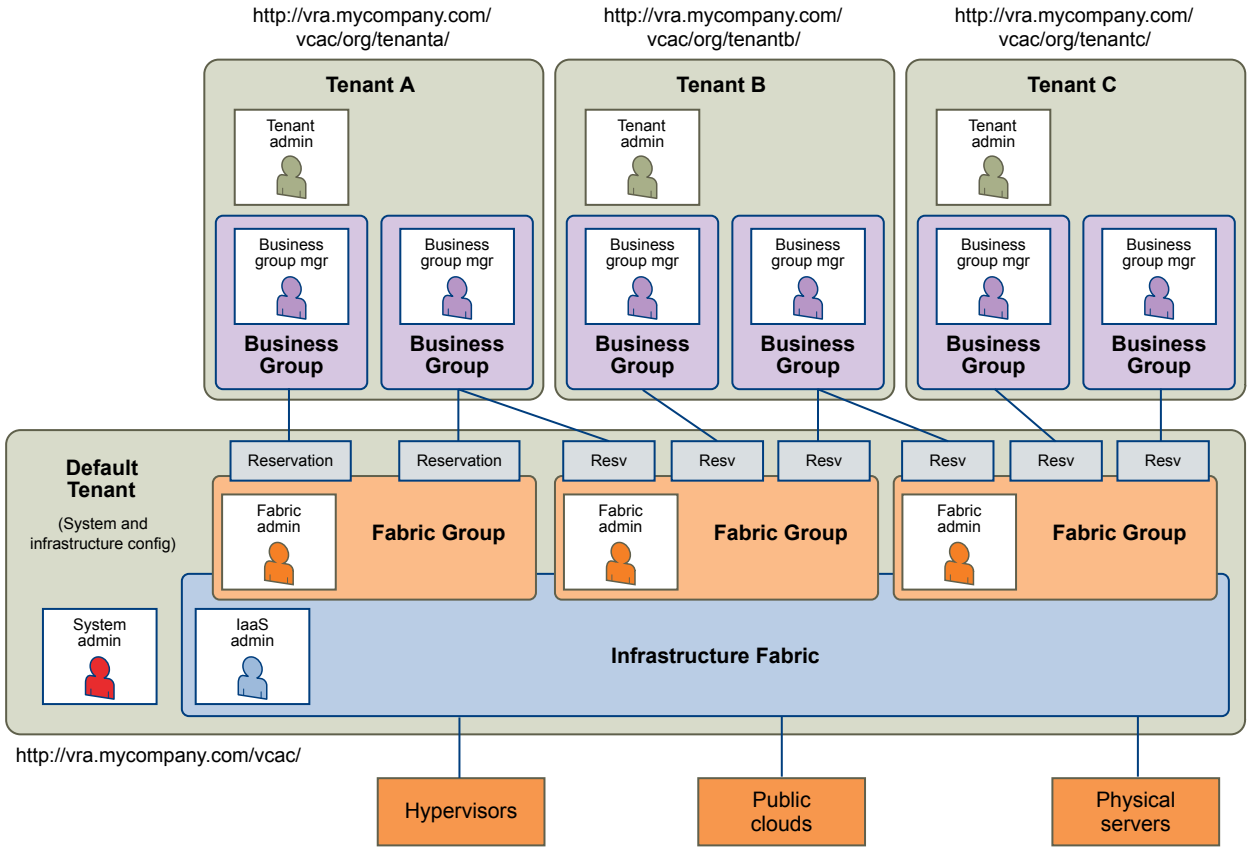
Table 8-2. Multitenant Deployment Examples

Example	Description
Manage infrastructure configuration only in the default tenant	In this example, all infrastructure is centrally managed by IaaS administrators and fabric administrators in the default tenant. The shared infrastructure resources are assigned to the users in each tenant by using reservations.
Manage infrastructure configuration in each tenant	In this scenario, each tenant manages its own infrastructure and has its own IaaS administrators and fabric administrators. Each tenant can provide its own infrastructure sources or can share a common infrastructure. Fabric administrators manage reservations only for the users in their own tenant.

The following diagram shows a multitenant deployment with centrally managed infrastructure. The IaaS administrator in the default tenant configures all infrastructure sources that are available for all tenants. The IaaS administrator can organize the infrastructure into fabric groups according to type and intended purpose. For example, a fabric group might contain all virtual resources, or all Tier One resources. The fabric administrator for each group can allocate resources from their fabric groups. Although the fabric administrators exist only in the default tenant, they can assign resources to business groups in any tenant.

Note Some infrastructure tasks, such as importing virtual machines, can only be performed by a user with both the fabric administrator and business group manager roles. These tasks might not be available in a multitenant deployment with centrally managed infrastructure.

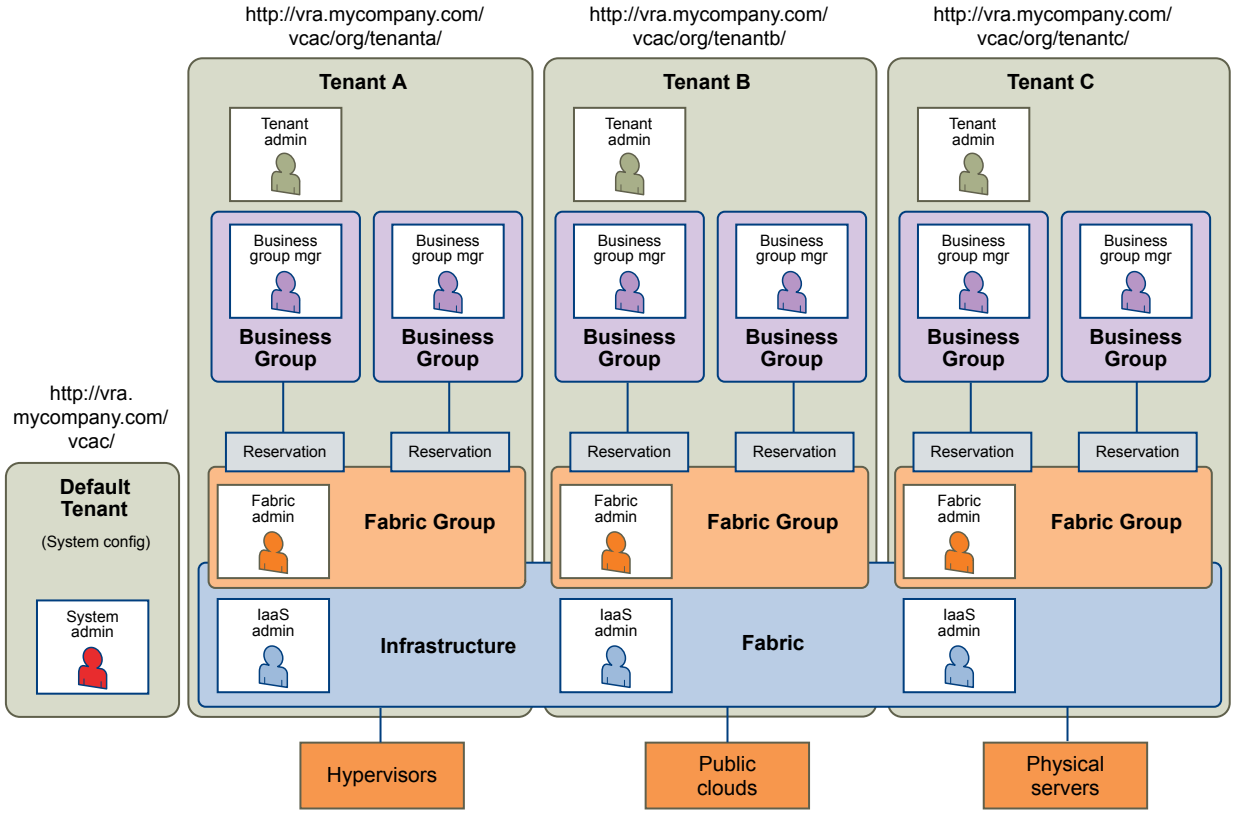
Figure 8-2. Multitenant Example with Infrastructure Configuration Only in Default Tenant



The following diagram shows a multitenant deployment where each tenant manages their own infrastructure. The system administrator is the only user who logs in to the default tenant to manage system-wide configuration and create tenants.

Each tenant has an IaaS administrator, who can create fabric groups and appoint fabric administrators with their respective tenants. Although fabric administrators can create reservations for business groups in any tenant, in this example they typically create and manage reservations in their own tenants. If the same identity store is configured in multiple tenants, the same users can be designated as IaaS administrators or fabric administrators in each tenant.

Figure 8-3. Multitenant Example with Infrastructure Configuration in Each Tenant



Create and Configure a Tenant

System administrators create tenants and specify basic configuration such as name, login URL, identity stores, and administrators.

Prerequisites

Log in to the vRealize Automation console as a **system administrator**.

Procedure

1 Specify Tenant Information

The first step to configuring a tenant is to name the new tenant and add it to vRealize Automation and create the tenant-specific access URL.

2 Configure Identity Stores

   Each tenant must be associated with at least one identity store. Identity stores can be OpenLDAP or Active Directory. Use of Native Active Directory is also supported for the default tenant.

3 Appoint Administrators

   You can appoint one or more tenant administrators and IaaS administrators from the identity stores you configured for a tenant.

Specify Tenant Information

The first step to configuring a tenant is to name the new tenant and add it to vRealize Automation and create the tenant-specific access URL.

Prerequisites

Log in to the vRealize Automation console as a **system administrator**.

Procedure

1 Select **Administration > Tenants**.

2 Click the **Add** icon ( ).

3 Enter a name in the **Name** text box.

4 (Optional) Enter a description in the **Description** text box.

5 Enter a unique identifier for the tenant in the **URL Name** text box.

   This URL token is used to append a tenant-specific identifier to the vRealize Automation console URL.

   For example, enter **`mytenant`** to create the URL https://*vrealize-appliance-hostname.domain.name*/vcac/org/*mytenant*.

6 (Optional) Enter an email address in the **Contact Email** text box.

7 Click **Submit and Next**.

Your new tenant is saved and you are automatically directed to the **Identity Stores** tab for the next step in the process.

Configure Identity Stores

Each tenant must be associated with at least one identity store. Identity stores can be OpenLDAP or Active Directory. Use of Native Active Directory is also supported for the default tenant.

Prerequisites

Specify Tenant Information.

Procedure

1. Click the **Add** icon ( ).
2. Enter a name in the **Name** text box.
3. Select the type of identity store from the **Type** drop-down menu.
4. Enter the URL for the identity store in the **URL** text box.

   For example, `ldap://ldap.mycompany.com:389` .
5. Enter the domain for the identity store in the **Domain** text box.
6. (Optional) Enter the domain alias in the **Domain Alias** text box.

   The alias allows users to log in by using *userid@domain-alias* rather than *userid@identity-store-domain* as a user name.
7. Enter the Distinguished Name for the login user in the **Login User DN** text box.

   Use the display format of the user name, which can include spaces and is not required to be identical to the user ID.

   For example, `cn=Demo Admin,ou=demo,dc=dev,dc=mycompany,dc=com`.
8. Enter the password for the identity store login user in the **Password** text box.
9. Enter the group search base Distinguished Name in the **Group Search Base DN** text box.

   For example, `ou=demo,dc=dev,dc=mycompany,dc=com`.
10. (Optional) Enter the user search base Distinguished Name in the **User Search Base DN** text box.

    For example, `ou=demo,dc=dev,dc=mycompany,dc=com`.
11. Click **Test Connection**.

    Check that the connection is working.
12. Click **Add**.
13. (Optional) Repeat Step 1 to Step 12 to configure additional identity stores.
14. Click **Next**.

Your new identity store is saved and associated with the tenant. You are directed to the **Administrators** tab for the next step in the process.

Appoint Administrators

You can appoint one or more tenant administrators and IaaS administrators from the identity stores you configured for a tenant.

Tenant administrators are responsible for configuring tenant-specific branding, as well as managing identity stores, users, groups, entitlements, and shared blueprints within the context of their tenant. IaaS Administrators are responsible for configuring infrastructure source endpoints in IaaS, appointing fabric administrators, and monitoring IaaS logs.

Prerequisites

- Configure Identity Stores.
- Before you appoint IaaS administrators, you must install IaaS. For more information about installation, see *Installation and Configuration*.

Procedure

1. Enter the name of a user or group in the **Tenant Administrators** search box and press Enter.

   For faster results, enter the entire user or group name, for example myAdmins@mycompany.domain. Repeat this step to appoint additional tenant administrators.

2. If you have installed IaaS, enter the name of a user or group in the **Infrastructure Administrators** search box and press Enter.

   For faster results, enter the entire user or group name, for example IaaSAdmins@mycompany.domain. Repeat this step to appoint additional infrastructure administrators.

3. Click **Add**.

Updating vRealize Automation Certificates

9

A system administrator can replace certificates for vRealize Automation components. Typically, you replace a certificate to switch from self-signed certificates to certificates provided by a certificate authority or when a certificate expires.

When you replace a certificate for a vRealize Automation component, components that have a dependency on this certificate are affected. You must register the new certificate with these components to ensure certificate trust.

You must update all components of the same type in a distributed system. For example, if you update a certificate for one vRealize Appliance in a distributed environment, you must update all instances of vRealize Appliance for that installation.

Certificates for the Identity Appliance management site and vRealize Appliance management site do not have registration requirements.

Note vRealize Automation supports both SHA1 and SHA2 certificates. The self-signed certificates generated by the system use SHA-256 With RSA Encryption. You may need to update vRealize Automation components to use SHA2 certificates due to browser requirements.

Update components in the following order:

1 Identity Appliance

2 vRealize Appliance

3 IaaS components

With one exception, changes to later components in this list do not affect earlier ones. For example, if you import a new certificate to a vRealize Appliance, you must register this change with the IaaS server, but not with the Identity Appliance. The exception is that an updated certificate for IaaS components must be registered with vRealize Appliance.

The following table shows registration requirements when you update a certificate.

Table 9-1. Registration Requirements

Updated Certificate	Register new certificate with Identity Appliance	Register new certificate with vRealize Appliance	Register new certificate with IaaS
Identity Appliance	Not applicable	Done automatically when you replace the vRealize Appliance certificate	Done automatically when you replace the vRealize Appliance certificate
vRealize Appliance	No	Not applicable	Yes
IaaS	No	Yes	Not applicable

Note If your certificate uses a passphrase for encryption and you do not enter it when you replace your certificate on the virtual appliance, the certificate replacement fails and the message `Unable to load private key` appears.

In addition to certificates for the Identity Appliance, the vRealize Appliance, IaaS Website components, and Manager Service components, your deployment can have certificates for the Identity Appliance management site and the vRealize Appliance management site. Management Agents also have certificates. Each IaaS machine runs a Management Agent.

For important information about troubleshooting, supportability, and trust requirements for certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2106583.

This chapter includes the following topics:

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 9-2. 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**

Updating the Identity Appliance Certificate

The system administrator can replace a self-signed certificate with another self-signed certificate or a domain certificate after the installation is complete.

1 Replace a Certificate in the Identity Appliance

The system administrator can replace a self-signed certificate with one from a certificate authority. The same certificate can be used on multiple machines.

2 Update the vRealize Appliance with the Identity Appliance Certificate

After the Identity Appliance certificate is updated, the system administrator updates the vRealize Appliance with the new certificate information. This process reestablishes trusted communications between the virtual appliances.

Replace a Certificate in the Identity Appliance

The system administrator can replace a self-signed certificate with one from a certificate authority. The same certificate can be used on multiple machines.

The labels for the private key and certificate chain headers and footers depend on the certificate authority in use. Information here is based on headers and footers for a certificate generated by `openssl`.

Procedure

1 Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.

2 Log in with user name **`root`** and the password you specified when you deployed the Identity Appliance.

3 Click the **SSO** tab.

The red text is a prompt, not an error message.

4 Select the certificate type from the **Choose Action** menu.

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

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Appliance and any load balancer by using Subject Alternative Name (SAN) certificates.

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

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

Option	Action
Import PEM Encoded Certificate	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. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the **Pass Phrase** text box.
Generate Self-Signed Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as **.mycompany*.com. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

5 Click **Apply Settings.**

The certificate is updated.

Update the vRealize Appliance with the Identity Appliance Certificate

After the Identity Appliance certificate is updated, the system administrator updates the vRealize Appliance with the new certificate information. This process reestablishes trusted communications between the virtual appliances.

Use the `import-certificate` command to import the SSL certificate from the Identity Appliance into the SSL keystore used by the vRealize Appliance. The `alias` value specifies the alias under which the imported certificate is stored in the keystore, and `url` is the address of the SSL endpoint.

Prerequisites

Replace a Certificate in the Identity Appliance.

Procedure

1 Start Putty or another Unix SSL remote login tool.

2 Log in to the vRealize Appliance with user name **root** and the password you specified when deploying the appliance.

3 Execute the `import-certificate` command:

/usr/sbin/vcac-config import-certificate --alias websso --url https://*identity-hostname.domain.name*:7444

For example:

/usr/sbin/vcac-config import-certificate --alias websso --url https://identity-vm76-115.eng.mycompany.com:7444

4 Restart the vRealize Appliance.

5 Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.

6 Select **System > Reboot**.

7 Click **Services** and wait for all services to be registered.

The certificate is updated on the vRealize Appliance.

Updating the vRealize Appliance Certificate

The system administrator can replace a self-signed certificate with another self-signed certificate or a domain certificate. You can use Subject Alternative Name (SAN) certificates, wildcard certificates, or any other method of multi-use certification appropriate for your environment as long as you satisfy the trust requirements.

1 Replace a Certificate in the vRealize Appliance

The system administrator can replace a self-signed certificate with a trusted one from a certificate authority. You can use Subject Alternative Name (SAN) certificates, wildcard certificates, or any other method of multi-use certification appropriate for your environment as long as you satisfy the trust requirements.

2 Update SSO Registration for the vRealize Appliance

When the host name for a vRealize Appliance is changed, the system administrator must update Identity Appliance SSO registration.

3 Update the IaaS Servers with the vRealize Appliance Certificate

After the virtual appliance certificates are updated, the system administrator updates the IaaS server running the Model Manager Data component registry to reestablish trusted communications between the virtual appliances and IaaS components.

Replace a Certificate in the vRealize Appliance

The system administrator can replace a self-signed certificate with a trusted one from a certificate authority. You can use Subject Alternative Name (SAN) certificates, wildcard certificates, or any other method of multi-use certification appropriate for your environment as long as you satisfy the trust requirements.

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Log in with user name **`root`** and the password you specified when deploying the Identity Appliance.
3. Navigate to **vRA Settings > Host Settings**.
4. Go to the **SSL Configuration** pane.

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 Appliance and any load balancer through the use of Subject Alternative Name (SAN) certificates.

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

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

Option	Action
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. 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.
Generate Certificate	a Type a common name for the self-signed certificate in the **Common Name** text box. You can use the fully qualified domain name of the virtual appliance (*hostname.domain.name*) or a wild card, such as *.*mycompany*.com. If you use a load balancer, you need to specify the FQDN of the load balancer or a wildcard that matches the name of the load balancer. If the name is the same as the host name for the virtual appliance, you can leave the text box empty. Do not accept a default value if one is shown, unless it matches the host name of the virtual appliance. b Type your organization name, such as your company name, in the **Organization** text box. c Type your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Type a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.

6 Click **Save Settings**.

After a few minutes, the certificate details appear on the page.

The certificate is updated.

Update SSO Registration for the vRealize Appliance

When the host name for a vRealize Appliance is changed, the system administrator must update Identity Appliance SSO registration.

Prerequisites

Replace a Certificate in the vRealize Appliance.

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Log in with user name **root** and the password you specified when deploying the Identity Appliance.
3. Go to **vRA Settings > SSO.**
4. Verify that the fully qualified name for the Identity Appliance, *identity-va-hostname.domain.name*, appears in the **SSO Host** text box.

   For example, **vra-sso.mycompany.com**.

   The https:// prefix is not used.
5. Verify that **:7444** is the entry in the **SSO Port** text box.
6. Verify that the SSO default tenant is **vsphere.local**.

   Do not change this name.
7. Type the default administrator name **administrator@vsphere.local** in the **SSO Admin User** text box.
8. Type the SSO administrator password in the **SSO Admin Password** text box.

   The password must match the password you specified in the SSO settings for the Identity Appliance.
9. Click **Save Settings**.

The Identity Appliance is updated with certificate information for the new vRealize Appliance host name.

Update the IaaS Servers with the vRealize Appliance Certificate

After the virtual appliance certificates are updated, the system administrator updates the IaaS server running the Model Manager Data component registry to reestablish trusted communications between the virtual appliances and IaaS components.

Execute the `vcac-Config.exe` command with the `UpdateServerCertificates` argument to update the IaaS database to recognize the new vRealize Appliance certificate.

For help on the `vcac-Config` command, type the following at a command prompt:

```
vcac-Config.exe help
```

Prerequisites

Update SSO Registration for the vRealize Appliance.

Procedure

1 Open a command prompt as an administrator and navigate to the `Cafe` directory on the Model Manager Data installation machine.

```
C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe
```

2 Type the following command to update the IaaS database with the certificate information in one step. Supply the IaaS database name (vcac, by default) and the fully qualified domain name of the database server.

```
vcac-Config.exe UpdateServerCertificates -d vcac_database -s sql_database_server -v
```

For example:

```
vcac-Config.exe UpdateServerCertificates -d vCAC -s tr-w2008-13.eng.mycompany -v
```

Note The version of the command shown here, without the thumbprint argument, downloads the certificate in one step.

3 (Optional) If you use self-signed certificates or certificates signed by a custom certificate authority (CA), verify that the Windows servers that host the Manager Service, DEMs, and IaaS Website trust the new certificate and its certificate chain.

4 (Optional) Add the virtual appliance certificate to the trusted store if it is not trusted and recheck that Windows servers now trust the certificate and its certificate chain.

5 Type **`iisreset`** to reset IIS.

For high-availability installations, reset IIS for all servers that are part of your installation.

Updating the IaaS Certificate

The system administrator can replace a self-signed certificate with another self-signed certificate or a certificate from a certificate authority after the installation is complete. Certificate updates are required when the certificate type changes or the certificate expires.

1 Replace the Internet Information Services Certificate

The system administrator can replace an expired certificate or a self-signed certificate with one from a certificate authority to ensure security in a distributed deployment environment.

2 Update the vRealize Appliance with the IaaS Certificate

After certificates are updated on the IaaS servers, the system administrator updates the component registry to reestablish trusted communications between the virtual appliances and IaaS components.

3 Update Guest Agent Trust Relationship

You may need to update the trust relationship between vRealize Automation and Guest Agents if you updated or replaced an IaaS certificate. Guest Agents run on the virtual machine template that is used for provisioning through vRealize Automation.

Replace the Internet Information Services Certificate

The system administrator can replace an expired certificate or a self-signed certificate with one from a certificate authority to ensure security in a distributed deployment environment.

You can use a Subject Alternative Name (SAN) certificate on multiple machines. Import the certificate to the trusted root certificate store of all machines on which you installed the Website Component and Manager Service (the IIS machines) during the IaaS installation.

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. Update IIS bindings.
   a. Select the site that hosts the component Web site and model manager.
   b. Click **Bindings** in the Action pane.
   c. Click **Edit** on the https (443) in the Site Bindings dialog box.
   d. Change the SSL certificate to the newly imported one.
9. Restart IIS or open an elevated command prompt window and type `iisreset`.

Update the vRealize Appliance with the IaaS Certificate

After certificates are updated on the IaaS servers, the system administrator updates the component registry to reestablish trusted communications between the virtual appliances and IaaS components.

As part of updating an IaaS certificate, you must register the new certificate with the vRealize Appliance. You can use the hostname or IP address of the IaaS machines in the following commands. If you are using a load balancer, supply the host name of the load balancer instead. Note that URL paths are case-sensitive.

If you encounter errors, see the troubleshooting section in the installation documentation.

Prerequisites

Replace the Internet Information Services Certificate.

Procedure

1 On the IaaS machine that has an updated certificate, open a command prompt as Administrator, and navigate to the following directory.

```
C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe
```

2 Register the address for applicable IaaS components by entering the following command:

```
Vcac-Config.exe RegisterEndpoint --EndpointAddress
https://<iaas-web-server-or-load-balancer-hostname> -v
```

For example:

```
Vcac-Config.exe RegisterEndpoint --EndpointAddress
https://vcac.tech.mycompany.com -v
```

3 Restart the vRealize Appliance service by entering the following command:

```
service vcac-server restart
```

Wait approximately 15 minutes for the service to restart.

Update Guest Agent Trust Relationship

You may need to update the trust relationship between vRealize Automation and Guest Agents if you updated or replaced an IaaS certificate. Guest Agents run on the virtual machine template that is used for provisioning through vRealize Automation.

You do not need to entirely reinstall Guest Agents in order to reestablish the trust relationship with vRealize Automation. The `cert.pem` file that resides on the machine on which the Guest Agent is installed contains the certificate trust data. In order to reestablish trust, this file must be updated.

The location of this file depends on whether the Guest Agent runs under Windows or Linux.

Table 9-3. Guest Agent Certificate File Locations

Operating System	Folder
Windows	`c:\vrmguestagent\cert.pem`
Linux	`/usr/share/gugent/cert.pem`

Update the `cert.pem` file by running the appropriate commands.

Prerequisites

- Obtain the server name and IP address of the server that runs the IaaS Manager Service.
- If necessary, convert the template on which the Guest Agent is installed to a virtual machine.

Procedure

1 Run the operating system appropriate commands in an elevated command prompt.

Option	Description
Windows	Run the following commands: a `cd c:\vrmguestagent` b `echo | openssl s_client –connect` *`manager_service_load_balancer.mycompany.com`*`:443 | sed –ne '/–BEGIN CERTIFICATE–/,/–END CERTIFICATE–/p' > cert.pem`
Linux	Run the following commands: a `cd /usr/share/gugent` b `echo | openssl s_client –connect` *`manager_service_load_balancer.mycompany.com`*`:443 | sed –ne '/–BEGIN CERTIFICATE–/,/–END CERTIFICATE–/p' > cert.pem`

2 If applicable, convert the Guest Agent virtual machine back to a template.

Replace the Identity Appliance Management Site Certificate

The Identity Appliance uses lighttpd to run its own management site. You can replace the SSL certificate of the management site service, for example, if your certificate expires or if you are using a self-signed certificate and your company security policy requires you to use its SSL certificates. You secure the management site service on port 5480.

Prerequisites

To install a new certificate, the certificate must be in PEM format and the private key cannot be encrypted. By default the Identity Appliance management site SSL certificate and private key are stored in a PEM file located at `/opt/vmware/etc/lighttpd/server.pem`.

See Extracting Certificates and Private Keys if you require information about exporting a certificate and private key from a Java keystore to a PEM file.

Procedure

1 Log in by using the appliance console or SSH.

2 Back up your current certificate file.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem–bak
```

3 Copy the new certificate to your appliance by replacing the content of the file `/opt/vmware/etc/lighttpd/server.pem` with the new certificate information.

4 Run the following command to restart the lighttpd server.

```
service vami-lighttp restart
```

5 Log in to the management console and validate that the certificate is replaced. You might need to restart your browser.

The new Identity Appliance management site certificate is installed.

Updating the vRealize Appliance Management Site Certificate

The system administrator can replace the SSL certificate of the management site service when it expires or to replace a self-signed certificate with one issued by a certificate authority. You secure the management site service on port 5480.

The vRealize Appliance uses lighttpd to run its own management site. When you replace a management site certificate, you must also configure all Management Agents to recognize the new certificate.

If you are running a distributed deployment, you can update Management Agents automatically or manually. If you are running a minimal deployment, you must update the management agent manually.

See Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate for more information.

1 Replace the vRealize Automation Appliance Management Site Certificate

The vRealize Appliance uses lighttpd to run its own management site. You can replace the SSL certificate of the management site service if your certificate expires or if you are using a self-signed certificate and your company security policy requires you to use its SSL certificates. You secure the management site service on port 5480.

2 Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate

After replacing a vRealize Appliance management site certificate, a system administrator updates all Management Agents to recognize the new certificate to reestablish trusted communications between the virtual appliance management site and Management Agents on IaaS hosts. Each IaaS hosts runs a Management Agent and each Management Agent must be updated.

3 Automatically Update Management Agents in a Distributed Environment to Recognize a vRealize Appliance Management Site Certificate

After the Management Site certificate is updated in a high-availability deployment, the Management Agent configuration must be modified so that it recognizes the new certificate. This is necessary to reestablish trusted communications between the virtual appliance management site and Management Agents on IaaS host. Each IaaS host runs a Management Agent and each Management Agent must be updated.

Replace the vRealize Automation Appliance Management Site Certificate

The vRealize Appliance uses lighttpd to run its own management site. You can replace the SSL certificate of the management site service if your certificate expires or if you are using a self-signed certificate and your company security policy requires you to use its SSL certificates. You secure the management site service on port 5480.

You can choose to install a new certificate or reuse the certificate used by the vCloud Automation Center service on port 443.

When you request a new certificate to update another CA-issued certificate, it is a best practice to reuse the Common Name from the existing certificate.

Prerequisites

- New certificates must be in PEM format and the private key cannot be encrypted. By default, the vRealize Appliance management site SSL certificate and private key are stored in a PEM file located at `/opt/vmware/etc/lighttpd/server.pem`.

  See Extracting Certificates and Private Keys if you require information about exporting a certificate and private key from a Java keystore to a PEM file.

Procedure

1. Log in by using the appliance console or SSH.
2. Back up your current certificate file.

   ```
   cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
   ```

3. Copy the new certificate to your appliance by replacing the content of the file `/opt/vmware/etc/lighttpd/server.pem` with the new certificate information.
4. Run the following command to restart the lighttpd server.

   ```
   service vami-lighttp restart
   ```

5. Log in to the management console and validate that the certificate is replaced. You might need to restart your browser.

The new vRealize Appliance management site certificate is installed.

What to do next

Update all management agents to recognize the new certificate.

For distributed deployments, you can update management agents manually or automatically. For minimal installations, you must update agents manually.

- For information about automatic update, see Automatically Update Management Agents in a Distributed Environment to Recognize a vRealize Appliance Management Site Certificate.

- For information about manual update, see Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate.

Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate

After replacing a vRealize Appliance management site certificate, a system administrator updates all Management Agents to recognize the new certificate to reestablish trusted communications between the virtual appliance management site and Management Agents on IaaS hosts. Each IaaS hosts runs a Management Agent and each Management Agent must be updated.

Perform these steps for each Management Agent in your deployment after you replace a certificate for the vRealize Appliance management site.

For distributed deployments, you can update Management Agents manually or automatically. For information about automatic update, see Automatically Update Management Agents in a Distributed Environment to Recognize a vRealize Appliance Management Site Certificate

For minimal deployments, you must update Management Agents manually as described in this procedure.

Prerequisites

Obtain the SHA1 thumbprints of the new vRealize Appliance management site certificate.

Procedure

1. Stop the VMware vCloud Automation Center Management Agent service.
2. Navigate to the Management Agent configuration file located at `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`, typically `C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
3. Open the file for editing and locate the endpoint configuration setting for the old management site certificate. which you can identify by the endpoint address.

   For example:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

4 Change the thumbprint to the SHA1 thumbprint of the new certificate.

For example:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

5 If there are other `managementEndpoint` entries, delete them.

6 Start the VMware vCloud Automation Center Management Agent service.

7 Login to the virtual appliance management site and go to**vRA Settings > Cluster**.

8 Check the Distributed Deployment Information table to verify that the IaaS server has contacted the virtual appliance recently, which confirms that the update is successful.

Automatically Update Management Agents in a Distributed Environment to Recognize a vRealize Appliance Management Site Certificate

After the Management Site certificate is updated in a high-availability deployment, the Management Agent configuration must be modified so that it recognizes the new certificate. This is necessary to reestablish trusted communications between the virtual appliance management site and Management Agents on IaaS host. Each IaaS host runs a Management Agent and each Management Agent must be updated.

You can update vRealize Appliance management site certificate information for distributed systems manually or automatically. For information about manually updating Management Agents, see Manually Update Management Agents to Recognize a vRealize Appliance Management Site Certificate.

Use this procedure to update the certificate information automatically.

Procedure

1 When Management Agents are running, replace the certificate on a single vRealize Appliance management site in your deployment.

2 Wait fifteen minutes for the Management Agent to synchronize with the new vRealize Appliance management site certificate.

3 Replace certificates on other vRealize Appliance management sites in your deployment.

Management Agents are automatically updated with the new certificate information.

Replace a Management Agent Certificate

The system administrator can replace the Management Agent certificate when it expires or replace a self-signed certificate with one issued by a certificate authority.

Each IaaS host runs its own Management Agent. Repeat this procedure on each IaaS node whose Management Agent you want to update.

Prerequisites

- Before you replace a Management Agent certificate, remove its entry from the Distributed Deployment Information table. Note the Management Agent identifier in the Node ID column before you remove the record. You use this identifier when you create the new Management Agent certificate and when you register it. For more information, see the procedure about removing a node from the Distributed Deployment Information table in *System Administration* for vRealize Automation.
- When you request a new certificate, ensure that the Common Name (CN) attribute in the certificate subject field for the new certificate is typed in in the following format:

  ```
  VMware Management Agent 00000000-0000-0000-0000-000000000000
  ```

  Use the string VMware Management Agent, followed by a single space and the GUID for the Management Agent in the numerical format shown.
- Record the SHA1 thumbprint of the new Management Agent certificate.

Procedure

1. Stop the Management Agent service from your Windows Services snap-in.
   a. From your Windows machine, click **Start**.
   b. In the Windows Start Search box, type **`services.msc`** and press Enter.
   c. Right-click **VMware vCloud Automation Center Management Agent** service and click **Stop** to stop the service.
2. Remove the current certificate from the machine. For information about managing certificates on Windows Server 2008 R2, see the Microsoft Knowledge Base article at http://technet.microsoft.com/en-us/library/cc772354.aspx or the Microsoft wiki article at http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx.

3 Register the Management Agent certificate with the vRealize Appliance management site.

a Open a command prompt as an administrator and navigate to the Cafe directory on the machine on which the Management Agent is installed at `<vra-installation-dir>\Management Agent\Tools\Cafe`, typically `C:\Program Files (x86)\VMware\vCAC\Management Agent\Tools\Cafe`

b Type the `Vcac-Config.exe RegisterNode` command with options to register the Management Agent identifier and certificate in one step. Include the Management Agent identifier you recorded earlier as the value for the `-nd` option and the thumbprint of the new certificate as the value of the `-tp`.

Table 9-4. Required Options and Arguments for Vcac-Config.exe RegisterNode

Option	Argument	Notes
`-url`	"*vra-va-hostname.domain.name*:5480"	The URL of the management site host, including a port specification
`-cu`	"root"	The user name, which must be the root user
`-cp`	"*password*"	Password for the root user as a quoted string
`-hn`	"*machine-hostname.domain.name*"	The machine name of the Management Agent host, including domain information
`-nd`	"*00000000-0000-0000-0000-000000000000*"	Management Agent identifier
`-tp`	"*0000000000000000000000000000000000000000*"	Thumbprint for the new certificate

The following example shows the command format:

```
Vcac-Config.exe RegisterNode -v -url "vra-va-hostname.domain.name:5480"
-cu "root" -cp "password" -hn "machine-hostname.domain.name"
-nd "00000000-0000-0000-0000-000000000000"
-tp "0000000000000000000000000000000000000000"
```

Example: Command to Register a Management Agent Certificate

`Vcac-Config.exe RegisterNode -v -url "vra-va.eng.mycompany:5480" -cu "root" -cp "secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp "70928851D5B72B206E4B1CF9F6ED953EE1103DED"`

Troubleshooting

10

vRealize Automation troubleshooting provides procedures for resolving issues you might encounter when installing or configuring vRealize Automation.

This chapter includes the following topics:

- Machine Requests Fail When Remote Transactions Are Disabled
- Credentials Error When Running the IaaS Installer
- Attempts to Log In as the IaaS Administrator with Incorrect UPN Format Credentials Fails with No Explanation
- Email Customization Behavior Has Changed
- Changes Made to /etc/hosts Files Might Be Overwritten
- Network Settings Were Not Successfully Applied

Default Log Locations

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

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

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

Windows Logs

Use the following location 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 by default.

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 located in the following places:

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`

Log	Default Location
Manager Service Logs	`C:\Program Files (x86)\VMware\vCAC\Server\Logs`
Orchestrator Logs	`C:\Program Files (x86)\VMware\vCAC\Distributed Execution Manager\DEO\Logs`
Worker DEM Logs	`C:\Program Files (x86)\VMware\vCAC\Distributed Execution Manager\DEM\Logs`
Agent Logs	`C:\Program Files (x86)\VMware\vCAC\Agents\<agent_name>\logs`

Identity Appliance Logs

You can generate a complete log file by creating a support bundle. See Create a Support Bundle for vRealize Automation.

Collection of Logs for Distributed Deployments

You can create a zip file that bundles all logs for components of a distributed deployment. See the topic on viewing host information for distributed deployments in the *System Administration* for vRealize Automation.

vRealize Automation Framework Logs

Log	Default location
Framework Logs	`C:\Program Files (x86)\VMware\vCAC\Distributed Execution Manager\DEO\Logs`

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 10-1. 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 Support Bundle for vRealize Automation

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

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

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

Procedure

1. Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.
2. Log in and go to **Admin > Logs**.
3. Click **Create support bundle**.
4. Click **Download** and save the file on your system.

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

Installers Fail to Download

Installers fail to download from the vRealize Appliance.

Problem

Installers do not download when running setup__*vra-va-hostname.domain.name*.exe.

Cause

- Network connectivity issues when connecting to the vRealize Appliance machine.
- Not able to connect to the vRealize 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 Appliance by typing the following URL in a Web browser.

   https://*vra-va-hostname.domain.name*

2 Check the other vRealize Appliance troubleshooting topics.

3 Download the setup file and reconnect to the vRealize Appliance.

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 Appliance or the Identity Appliance or connectivity issues between the appliances. A connection attempt fails because there was no response or the connection could not be made.
- Trusted certificate issues in IaaS when using a distributed configuration.
- A certificate name mismatch in a distributed configuration.
- The certificate may be invalid or an error on the certificate chain might exist.
- The Repository Service fails to start.
- Incorrect configuration of the load balancer in a distributed environment.

Solution

- Connectivity

  Check that you can connect to the vRealize Appliance by typing the following URL in a Web browser: https//*vra-va-hostname.domain.name*.

- Trusted Certificate Issues
  - In IaaS, open Microsoft Management Console with the command `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 browser, check https://<*ip-web*>/repository/data/MetaModel.svc and verify that no certificate errors appear in your browser.

- Certificate Name Mismatch

  This error can occur when the certificate is issued to a particular name and a different name or IP address is used. You can suppress the certificate name mismatch error during installation by selecting **Suppress certificate mismatch**.

  You can also use the Suppress certificate mismatch option to ignore remote certificate revocation list match errors.

- Invalid Certificate

  Open Microsoft Management Console with the command `mmc.exe`. Check that the certificate is not expired and that the status is correct. Do this for all certificates in the certificate chain. You might have to import other certificates in the chain into the Trusted Root Certificate Store when using a Certificate hierarchy.

- Repository Service

  Perform the following actions to check the status of the repository service.

  - From a browser, check the status of the MetaModel service at https://<*ip-web*>/repository/data/MetaModel.svc.
  - Check the `Repository.log` for errors.
  - Reset IIS (`iisreset`) if you have problems with the applications hosted on the Web site (Repository, vRealize Automation, or WAPI).
  - Check the Web site logs in *%SystemDrive%*`\inetpub\logs\LogFiles` for additional logging information.
  - Verify that Prerequisite Checker passed when checking the requirements.
  - On Windows 2012, check that WCF Services under .NET Framework is installed and that HTTP activation is installed.

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.

WAPI and Distributed Execution Managers Fail to Install

Your installation of vRealize Appliance WAPI 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 Appliance Distributed Execution Managers (DEMs) and WAPI 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.

Installation or Upgrade Fails with a Load Balancer Timeout Error

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

Problem

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.

Cause

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

Solution

1. Increase your load balancer timeout value to at least 100 seconds. For example, and depending on the load balancer you are using, edit the load balancer timeout setting in your `ssl.conf`, `httpd.conf` or other Web configuration file.
2. Rerun the installation or upgrade.

Uninstalling a Proxy Agent Fails

Removing a proxy agent can fail if Windows Installer Logging is enabled.

Problem

When you try to uninstall a proxy agent from the Windows Control Panel, the uninstall fails and you see the following error:

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

Cause

This can occur if Windows Installer Logging is enabled, but the Windows Installer engine cannot properly write the uninstallation log file. For more information, see the Microsoft Knowledge Base article at http://support.microsoft.com/kb/2564571.

Solution

1. Restart your machine or restart explorer.exe from the Task Manager.
2. Uninstall the agent.

Validating Server Certificates for IaaS

You can use the vcac-Config.exe command to verify that an IaaS server accepts vRealize 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.

Server Times Are Not Synchronized

An installation might not succeed when IaaS time servers are not synchronized with the vRealize Appliance and the Identity Appliance.

Problem

You cannot log in after installation, or the installation fails while it is completing.

Cause

Time servers on all servers might not be synchronized.

Solution

For each server (Identity Appliance, vRealize Appliance, and all Windows servers where the IaaS components will be installed), enable time synchronization as described in the following topics:

- Enable Time Synchronization on the Identity Appliance
- Enable Time Synchronization on the vRealize Appliance
- Enable Time Synchronization on the Windows Server

For an overview of timekeeping for vRealize Automation, see Time Synchronization.

RabbitMQ Configuration Fails in a High-Availability Environment

When RabbitMQ is restarted in a high-availability environment, vRealize Automation appliances must be shut down and restarted in a specified order.

Problem

Restart of RabbitMQ for vRealize Automation in a high-availability environment fails.

Cause

vRealize Automation appliances must be shut down and restarted in a specified order.

Solution

The last vRealize Automation appliance that is shut down or stopped should be the first to be started (or within 30 seconds of starting the second. The rabbitmq service on the other vRealize Automation appliance waits 30 seconds for the rabbitmq service on the last stopped appliance to start before it fails. If last stopped vRealize Automation appliance cannot be started, then reset rabbitmq on the other vRealize Automation appliance by running **`ssh script:vcac-vami rabbitmq-cluster-config reset_rabbitmq_node`**.

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 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.

Log in to the vRealize Automation Console Fails

Your installation appears to have completed successfully, but you cannot log in to the console.

Problem

You cannot log in to the vRealize Automation console at https://*vcac-va-hostname*/vcac.

Cause

Multiple conditions can prevent you from logging in to vRealize Automation console.

For example, the machine from which the user authenticates using Windows Authentication must be joined to the domain in which the vRealize Automation Identity Appliance is configured. See User Accounts and Credentials Required for Installation.

Solution

1 Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.

2 Log in and select **System > Reboot** to reboot the appliance.

3 Navigate to the vRealize Appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.

4 Log in and select **System > Reboot** to reboot the appliance.

You can also check the status of the services under the SSO tab in the vRealize Automation console or log in to the appliance and run `tail –f /var/vcac/log/catalina.out`.

Error Communicating to the Remote Server

An error message indicating a communication problem between the vRealize Appliance and the Identity Appliance appears when a problem exists in **Common Name**.

Problem

`Error Communicating to the Remote Server` error message appears when you configure the SSO from the vRealize Appliance management console, even when the configuration is correct and the virtual appliances are communicating successfully.

Cause

The **Common Name** or the alternative names in the Identity SSL certificate do not match the hostname in the SSO URL you entered in the vRealize Appliance.

Solution

1. In the Identity Appliance management console, replace the SSL certificate, making sure you enter as common name exactly the same FQDN (no protocol or port included) as it is accessed from vRealize Appliance.
2. Navigate to the Identity Appliance management console by using its fully qualified domain name, https://*identity-hostname.domain.name*:5480/.
3. Replace the SSL certificate and type the fully qualified domain name of the SSO host (as it is accessed from the vRealize Appliance) in the **Common Name** text box.

   Do not include the **`https://`** prefix or the port number.

Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7

When you use Internet Explorer 9 or 10 on Windows 7 and compatibility mode is enabled, some pages appear to have no content.

Problem

When using Internet Explorer 9 or 10 on Windows 7, the following pages have no content:

- Infrastructure
- Default Tenant Folder on the Orchestrator page
- Server Configuration on the Orchestrator page

Cause

The problem could be related to compatibility mode being enabled. You can disable compatibility mode for Internet Explorer with the following steps.

Solution

Prerequisites

Ensure that the menu bar is displayed. If you are using Internet Explorer 9 or 10, press Alt to display the Menu bar (or right-click the Address bar and then select **Menu bar**).

Procedure

1. Select **Tools > Compatibility View settings**.
2. Deselect **Display intranet sites in Compatibility View**.
3. Click **Close**.

Cannot Establish Trust Relationship for the SSL/TLS Secure Channel

You might receive the message "Cannot establish trust relationship for the SSL/TLS secure channel when upgrading security certificates for vCloud Automation Center."

Problem

If a certificate issue occurs with vcac-config.exe when upgrading a security certificate, you might see the following message:

```
The underlying connection was closed: Could not establish trust relationship
for the SSL/TLS secure channel
```

You can find more information about the cause of the issue by using the following procedure.

Solution

1. Open the `vcac-config.exe.config` file and locate the repository address : <add key="repositoryAddress" value=" https://[IaaS address]:443/repository/" />
2. Browse to the address with Internet Explorer.
3. Continue through any error messages about certificate trust issues.
4. Obtain a security report from Internet Explorer and use it to troubleshoot why this certificate is not trusted.

If problems persist, repeat the procedure by browsing with the address that needs to be registered, the Endpoint address that you used to register with vcac-config.exe.

Cannot Log in to a Tenant or Tenant Identity Stores Disappear

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

Problem

- When you log in to a tenant, you see a blank page displayed with a Submit button in the upper left-hand corner.
- You receive a System Exception error when accessing the tenant ID store configuration page.
- The ID store configuration disappears.

- You cannot log in to a tenant by using an LDAP account.
- The `catalina.out` log located in `/var/log/vmware/vcac/` shows an error similar to the following:

  ```
  12:40:49,190 [tomcat-http--34] [authentication] INFO
  com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl
  $RequestResponseProcessor.handleFaultCondition:922 - Failed trying to retrieve
  token: ns0:RequestFailed: Error occurred looking for solution user ::
  Insufficient access YYYY-03-18 12:40:49,201 [tomcat-http--34] [authentication]
  ERROR
  com.vmware.vcac.platform.service.rest.resolver.ApplicationExceptionHandler.handle
  UnexpectedException:820 - Failed trying to retrieve token: ns0:RequestFailed:
  Error occurred looking for solution user :: Insufficient access
  com.vmware.vim.sso.client.exception.InternalError: Failed trying to retrieve
  token: ns0:RequestFailed: Error occurred looking for solution user ::
  Insufficient access
  ```

- The Identity Appliance `messages` log located in `/var/log/` shows an error message similar to the following:

  ```
  T16:50:18-05:00 lsassd[2913]: GSSAPI Error: The referenced context has expired
  (Unknown error) T08:34:41-06:00 vmdird: t@139870073485056: Lockout policy check -
  password expired. (cn=tenantadmin,cn=users,dc=tenant) T11:58:03-06:00
  lsassd[2943]: GSSAPI Error: The referenced context has expired (Unknown
  error)....
  ```

  ```
  Account "cn=tenantadmin,cn=users,dc=qic" password expired and caused login/bind
  from IDM to fail. YYYY-03-18T11:38:46-06:00 denqca3vcacid01 vmdird:
  t@140689332778752: LoginBlocked DN (cn=tenantadmin,cn=users,dc=tenant), error
  (9239)(Account access blocked)
  ```

Cause

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

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

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

Adding an Endpoint Causes an Internal Error

When you attempt to create an advanced services 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.

Cause

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.

Error in Manager Service Communication

IaaS nodes that are cloned from a template on which MS DTC is installed contain duplicate identifiers for MS DTC, which prevents communication among the nodes.

Problem

The IaaS Manager Service fails and displays the following error in the manager service log.

```
Communication with the underlying transaction manager has failed. ---->
System.Runtime.InteropServices.COMException: The MSDTC transaction manager was
unable to pull the transaction from the source transaction manager due to
communication problems. Possible causes are: a firewall is present and it
doesn't have an exception for the MSDTC process, the two machines cannot
find each other by their NetBIOS names, or the support for network transactions
is not enabled for one of the two transaction managers.
```

Cause

When you clone an IaaS node that has MS DTC installed, then both clones use the same unique identifier for MS DTC. Communication between the nodes fails.

Solution

1. Open an Administrator command prompt.
2. Run the following command: **`msdtc –uninstall`**
3. Reboot the virtual machine.

4 Open a separate command prompt and run the following command:
`msdtc –install <manager–service–host>`.

Machine Requests Fail When Remote Transactions Are Disabled

Machine requests fail when Microsoft Distributed Transaction Coordinator (DTC) remote transactions are disabled on Windows server machines.

Problem

If you provision a machine when remote transactions are disabled on the Model Manager portal or the SQL Server, the request will not complete. Data collection fails and the machine request remains in a state of CloneWorkflow.

Cause

DTC Remote Transactions are disabled in the IaaS SQL Instance used by the vRealize Automation system.

Solution

1 Launch Windows Server Manager to enable DTC on all vRealize servers and associated SQL servers.

In Windows 7, navigate **Start > Administrative Tools > Component Services**.

Note Ensure that all Windows servers have unique SIDs for MSDTC configuration.

2 Open all nodes to locate the local DTC, or the clustered DTC if using a clustered system.

Navigate **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

3 Right click on the local or clustered DTC and select **Properties**.

4 Click the Security tab.

5 Select the **Network DTC Access** option.

6 Select the **Allow Remote Client** and **Allow Remote Administration** options.

7 Select the **Allow Inbound** and **Allow Outbound** options.

8 Enter or select NT AUTHORITY\Network Service in the **Account** field for the DTC Logon Account.

9 Click **OK**.

10 Remove machines that are stuck in the Clone Workflow state.

a Log in to the vRealize Appliance.

https://*virtualappliancename*/vcac/*tenantname*

b Navigate to **Infrastructure > managed Machines**.

c Right click on the target machine.

d Select **Delete** to remove the machine.

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.

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.

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. For more information about configuring notifications, see Configuring Notifications in the VMware vCloud Automation Center 6.2 Documentation Center.

Changes Made to /etc/hosts Files Might Be Overwritten

Problem

If you made changes to the `/etc/hosts` file, they might be overwritten when any of the following actions occur:

- Reboot
- Network changes
- Changes made in the **Management console-> Network** tab
- Upgrade

Solution

To make a permanent change to the /etc/hosts file, you must make the change outside of the VAMI_EDIT_BEGIN to VAMI_EDIT_END section because this section is overwritten when a network change is detected.

Network Settings Were Not Successfully Applied

An error message that indicates a network problem appears in the console of a newly deployed Identity Appliance.

Problem

When you deploy the Identity Appliance in vSphere and select the option for a fixed IP address, you enter the IP address, default gateway, netmask value, and domain name server.

If the virtual appliance starts while the network is unavailable, however, the settings might not be successfully applied, and `No Networking Detected` appears on the console screen of the virtual appliance.

Solution

After deploying the Identity Appliance with a fixed IP address, log in to the virtual appliance console, and use the following command to configure the network settings.

```
/opt/vmware/share/vami/vami_config_net
```