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
## Contents

1 Installing or Upgrading vRealize Automation 4
   vRealize Automation Reference Architecture 4
   Initial Deployment and Configuration Recommendations 4
   vRealize Automation Deployment 5
   vRealize Business for Cloud Deployment Considerations 7
   vRealize Automation Scalability 7
   vRealize Business for Cloud Scalability 10
   vRealize Automation High Availability Configuration Considerations 10
   vRealize Business for Cloud High Availability Considerations 12
   vRealize Automation Hardware Specifications and Capacity Maximums 13
   vRealize Automation Small Deployment Requirements 15
   vRealize Automation Medium Deployment Requirements 20
   vRealize Automation Large Deployment Requirements 25
   vRealize Automation Multi-Data Center Data Deployments 31

vRealize Automation Secure Configuration 32
   vRealize Automation Secure Baseline Overview 32
   Verifying the Integrity of Installation Media 33
   Hardening VMware System Software Infrastructure 34
   Reviewing Installed Software 35
   VMware Security Advisories and Patches 36
   Secure Configuration 36
   Configuring Host Network Security 68
   Auditing and Logging 83

Installing vRealize Automation 83
   vRealize Automation Installation Overview 83
   Preparing for vRealize Automation Installation 91
   Deploying the vRealize Automation Appliance 107
   Installing vRealize Automation with the Installation Wizard 112
   The Standard vRealize Automation Installation Interfaces 136
   Silent vRealize Automation Installation 211
   vRealize Automation Post-Installation Tasks 217
   Troubleshooting a vRealize Automation Installation 235

Upgrading vRealize Automation 261
   Upgrading from vRealize Automation 7.1 or Greater to 7.4 264
   Upgrading vRealize Automation 6.2.5 to 7.4 390
   Migrating to vRealize Automation 7.4 471
Installing or Upgrading vRealize Automation

You can install vRealize Automation for the first time, or you can upgrade your current environment to the latest version.

This chapter includes the following topics:
- vRealize Automation Reference Architecture
- vRealize Automation Secure Configuration
- Installing vRealize Automation
- Upgrading vRealize Automation

vRealize Automation Reference Architecture
Reference architecture describes the structure and configuration of typical vRealize Automation deployments. In addition, it provides information about high availability, scalability and deployment profiles.

Reference architecture includes information about the following components:
- VMware vRealize Automation
- VMware vRealize Business for Cloud

For software requirements, installations, and supported platforms, see the documentation for each product.

Initial Deployment and Configuration Recommendations
Deploy and configure all VMware vRealize Automation components in accordance with VMware recommendations.

Keep your vRealize Automation, vRealize Business for Cloud, and vRealize Orchestrator in the same time zone with their clocks synchronized.

Install vRealize Automation, vRealize Business for Cloud, and vRealize Orchestrator on the same management cluster. Provision machines to a cluster that is separate from the management cluster so that user workload and server workload can be isolated.
Deploy Proxy Agents in the same data center as the Endpoint with which they communicate. VMware does not recommend placing DEM Workers in Remote Data Centers unless there is an express workflow skill-based use case that requires it. All components except the Proxy Agents and DEM Workers must be deployed in the same Data Center or Data Centers within a Metro Area Network. Latency must be less than 5 milliseconds, and bandwidth must not be less than 1 GB/s between the Data Centers in the Metro Area Network.

For more information including a support statement, see the VMware Knowledge Base article Installing the VMware vRealize Automation on a distributed multi-site instance available at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=213484.2.

vRealize Automation Deployment

Use the VMware resource recommendations as a starting point for vRealize Automation deployment planning.

After initial testing and deployment to production, continue to monitor performance and allocate additional resources if necessary, as described in vRealize Automation Scalability.

Authentication

When configuring vRealize Automation, you can use the default Directories Management connector for user authentication, or you can specify a pre-existing SAML based identity provider to support a single-sign on experience.

If two-factor authentication is required vRealize Automation supports integration with RSA SecurID. When this integration point is configured, users are prompted for their user ID and passcode.

Load Balancer Considerations

Use the Least Response Time or round-robin method to balance traffic to the vRealize Automation appliances and infrastructure Web servers. Enable session affinity or the sticky session feature to direct subsequent requests from each unique session to the same Web server in the load balancer pool.

You can use a load balancer to manage failover for the Manager Service, but do not use a load-balancing algorithm, because only one Manager Service is active at a time. Also, do not use session affinity when managing failover with a load balancer.

Use ports 443 and 8444 when load balancing the vRealize Automation Appliance. For the Infrastructure Website and Infrastructure Manager Service, only port 443 should be load balanced.

Although you can use other load balancers, NSX, F5 BIG-IP hardware, and F5 BIG-IP Virtual Edition are tested and are recommended for use.

See the vRealize Automation documentation for detailed information on configuring load balancers.
Database Deployment

vRealize Automation automatically clusters the appliance database in 7.0 and later releases. All new 7.0 and later deployments must use the internal appliance database. vRealize Automation instances which are upgrading to 7.1 or later must merge their external databases into the appliance database. See the vRealize Automation product documentation for more information on the upgrade process.

For production deployments of the Infrastructure components, use a dedicated database server to host the Microsoft SQL Server (MSSQL) databases. vRealize Automation requires machines that communicate with the database server to be configured to use Microsoft Distributed Transaction Coordinator (MSDTC). By default, MSDTC requires port 135 and ports 1024 through 65535.

For more information about changing the default MSDTC ports, see the Microsoft Knowledge Base article Configuring Microsoft Distributed Transaction Coordinator (DTC) to work through a firewall available at https://support.microsoft.com/en-us/kb/250367.

The IaaS Manager Service host must be able to resolve the NETBIOS name of the IaaS SQL Server database host. If it cannot resolve the NETBIOS name, add the SQL Server NETBIOS name to the Manager Service machine /etc/hosts file and restart the Manager Service.

vRealize Automation supports SQL AlwaysOn groups only with Microsoft SQL Server 2016. When installing SQL Server 2016, the database must be created in 100 mode. If you use an older version of Microsoft SQL Server, use a Failover Cluster instance with shared disks. For more information on configuring SQL AlwaysOn groups with MSDTC, see https://msdn.microsoft.com/en-us/library/ms366279.aspx.

Data Collection Configuration

The default data collection settings provide a good starting point for most implementations. After deploying to production, continue to monitor the performance of data collection to determine whether you must make any adjustments.

Proxy Agents

For maximum performance, deploy agents in the same data center as the endpoint to which they are associated. You can install additional agents to increase system throughput and concurrency. Distributed deployments can have multiple agent servers that are distributed around the globe.

When agents are installed in the same data center as their associated endpoint, you can see an increase in data collection performance of 200 percent, on average. The collection time measured includes only the time spent transferring data between the proxy agent and the manager service. It does not include the time it takes for the manager service to process the data.

For example, you currently deploy the product to a data center in Palo Alto and you have vSphere endpoints in Palo Alto, Boston, and London. In this configuration, the vSphere proxy agents are deployed in Palo Alto, Boston, and London for their respective endpoints. If instead, agents are deployed only in Palo Alto, you might see a 200 percent increase in data collection time for Boston and London.
Distributed Execution Manager Configuration

In general, locate distributed execution managers (DEMs) as close as possible to the model manager host. The DEM Orchestrator must have strong network connectivity to the model manager at all times. By default, the installer places DEM Orchestrators alongside the Manager Service. Create two DEM Orchestrator instances, one for failover, and two DEM Worker instances in your primary data center.

If a DEM Worker instance must run a location-specific workflow, install the instance in that location.

Assign skills to the relevant workflows and DEMs so that those workflows are always run by DEMs in the correct location. For information about assigning skills to workflows and DEMs by using the vRealize Automation designer console, see the vRealize Automation Extensibility documentation.

For the best performance, install DEMs and agents on separate machines. For additional information about installing vRealize Automation agents, see Installing Agents.

vRealize Orchestrator

Use the internal vRealize Orchestrator instance for all new deployments. If necessary, legacy deployments can continue to use an external vRealize Orchestrator. See https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109 for the procedure to increase the memory allocated to the internal vRealize Orchestrator instance.

For best product performance, review and implement configuration guidelines described in the vRealize Orchestrator Coding Design Guide prior to importing vRealize Orchestrator content into production deployments.

vRealize Business for Cloud Deployment Considerations


Load Balancer Considerations

Load balancing is not supported for data collection connections. For more information, see vRealize Automation Scalability. In the vRealize Business for Cloud appliance for user interface and API client connections, you can use the vRealize Automation load balancer.

vRealize Automation Scalability

Consider all applicable scalability factors when configuring your vRealize Automation system.

Users

The vRealize Automation appliance is configured for syncing less than 100,000 users. If your system contains more users, you may need to add memory to vRealize Automation Directories Management. For detailed information on adding memory to Directories Management, see Add Memory to Directories Management.
Concurrent Provisions Scalability

By default, vRealize Automation processes only eight concurrent provisions per endpoint. For information about increasing this limit, see Configuring Concurrent Machine Provisioning.

VMware recommends that all deployments start with at least two DEM-Workers. In 6.x each DEM-Worker could process 15 workflows concurrently. This was increased to 30 for vRealize Automation 7.0 and later.

If machines are being customized through Workflow Stubs, you should have 1 DEM-Worker per 20 Machines that will be provisioned concurrently. For example, a system supporting 100 concurrent provisions should have a minimum of 5 DEM-Workers.

For more information on DEM-Workers and scalability see Distributed Execution Manager Performance Analysis and Tuning

Data Collection Scalability

Data collection completion time depends on the compute resource capacity, the number of machines on the compute resource or endpoint, the current system, and network load, among other variables. The performance scales at a different rate for different types of data collection.

Each type of data collection has a default interval that you can override or modify. Infrastructure administrators can manually initiate data collection for infrastructure source endpoints. Fabric administrators can manually initiate data collection for compute resources. The following values are the default intervals for data collection.

<table>
<thead>
<tr>
<th>Data Collection Type</th>
<th>Default Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Every 24 hours (daily)</td>
</tr>
<tr>
<td>State</td>
<td>Every 15 minutes</td>
</tr>
<tr>
<td>Performance</td>
<td>Every 24 hours (daily)</td>
</tr>
</tbody>
</table>

Performance Analysis and Tuning

As the number of resources collecting data increases, data collection completion times might become longer than the interval between data collection intervals, particularly for state data collection. To determine whether data collection for a compute resource or endpoint is completing in time or is being queued, see the Data Collection page. The Last Completed field value might show In queue or In progress instead of a timestamp when data collection last finished. If this problem occurs, you can increase the interval between data collections to decrease the data collection frequency.

Alternatively, you can increase the concurrent data collection limit per agent. By default, vRealize Automation limits concurrent data collection activities to two per agent and queues requests that exceed this limit. This limitation allows data collection activities to finish quickly without affecting overall performance. You can raise the limit to take advantage of concurrent data collection, but you must weigh this option against overall performance degradation.
If you increase the configured vRealize Automation per-agent limit, you might want to increase one or more of these execution timeout intervals. For more information about how to configure data collection concurrency and timeout intervals, see the vRealize Automation System Administration documentation.

Manager Service data collection is CPU-intensive. Increasing the processing power of the Manager Service host can decrease the time required for overall data collection.

Data collection for Amazon Elastic Compute Cloud (Amazon AWS), in particular, can be CPU intensive, especially if your system collects data on multiple regions concurrently and if data was not previously collected on those regions. This type of data collection can cause an overall degradation in Web site performance. Decrease the frequency of Amazon AWS inventory data collection if it is having a noticeable effect on performance.

**Workflow Processing Scalability**

The average workflow processing time, from when the DEM Orchestrator starts preprocessing the workflow to when the workflow finishes executing, increases with the number of concurrent workflows. Workflow volume is a function of the amount of vRealize Automation activity, including machine requests and some data collection activities.

**Configure Manager Service for High Data Volume**

If you expect to use a VMware vSphere cluster that contains a large number of objects, for example, 3000 or more virtual machines, modify the manager service config file with larger values. If you do not modify this setting, large inventory data collections might fail.

Modify the default value of the ProxyAgentServiceBinding and maxStringContentLength settings in the ManagerService.exe.config file.

**Procedure**

1. Open the ManagerService.exe.config file in a text editor. Typically, this file resides at C:\Program Files (x86)\VMware\vCAC\Server.

2. Locate the binding name and readerQuotas lines in the file.

   ```xml
   <binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
     <readerQuotas maxStringContentLength="13107200" />
   </binding>
   ```

   **Note** Do not confuse these two lines with the similar lines that contain the following string: `binding name = "ProvisionServiceBinding"`.

3. Replace the number values assigned to the maxReceivedMessageSize and maxStringContentLength attributes with a larger value.

   The optimal size depends on how many more objects you expect your VMware vSphere cluster to contain in the future. For example, you can increase these numbers by a factor of 10 for testing.

4. Save your changes and close the file.

5. Restart the vRealize Automation manager service.
Distributed Execution Manager Performance Analysis and Tuning

You can view the total number of in progress or pending workflows at any time on the Distributed Execution Status page, and you can use the Workflow History page to determine how long it takes to run a given workflow.

If you have a large number of pending workflows, or if workflows are taking longer than expected to finish, add more Distributed Execution Manager (DEM) Worker instances to pick up the workflows. Each DEM Worker instance can process 30 concurrent workflows. Excess workflows are queued for execution.

You can adjust workflow schedules to minimize the number of workflows that start simultaneously. For example, rather than scheduling all hourly workflows to run at the beginning of the hour, you can stagger their run times so that they do not compete for DEM resources. For more information about workflows, see the vRealize Automation Extensibility documentation.

Some workflows, particularly certain custom workflows, can be CPU intensive. If the CPU load on the DEM Worker machines is high, consider increasing the processing power of the DEM machine or adding more DEM machines to your environment.

vRealize Business for Cloud Scalability

Configure your vRealize Business for Cloud installation for scalability in accordance with VMware guidelines.

vRealize Business for Cloud can scale up to 20,000 virtual machines across ten VMware vCenter Server instances. The first synchronization of the inventory data collection takes approximately three hours to synchronize 20,000 virtual machines across three VMware vCenter Server instances. Synchronization of statistics from VMware vCenter Server takes approximately one hour for 20,000 virtual machines. By default, the cost calculation job runs every day and takes approximately two hours for each run for 20,000 virtual machines.

Note In vRealize Business for Cloud 1.0, the default virtual appliance configuration can support up to 20,000 virtual machines. Increasing the limits of the virtual appliance beyond its default configuration does not increase the number of virtual machines that it can support.

vRealize Automation High Availability Configuration Considerations

If you require maximum system robustness, configure your vRealize Automation system for high availability in accordance with VMware guidelines.
vRealize Automation Appliance

The vRealize Automation appliance supports active-active high availability for all components except the appliance database. Starting with the 7.3 release, database failover is automatic if three nodes are deployed and synchronous replication is configured between two nodes. When vRealize Automation appliance detects database failure, it promotes a suitable database server to be the master. You can monitor and manage the appliance database on the Virtual Appliance Management Console vRA Settings > Database tab.

To enable high availability for these appliances, place them under a load balancer. For more information, see Configuring Your Load Balancer. Beginning with the 7.0 release, the appliance database, and vRealize Orchestrator are automatically clustered and available for use.

vRealize Automation Directories Management

Each vRealize Automation appliance includes a connector that supports user authentication, although only one connector is typically configured to perform directory synchronization. It does not matter which connector you choose to serve as the sync connector. To support Directories Management high availability, you must configure a second connector that corresponds to your second vRealize Automation appliance, which connects to your Identity Provider and points to the same Active Directory. With this configuration, if one appliance fails, the other takes over management of user authentication.

In a high availability environment, all nodes must serve the same set of Active Directories, users, authentication methods, etc. The most direct method to accomplish this is to promote the Identity Provider to the cluster by setting the load balancer host as the Identity Provider host. With this configuration, all authentication requests are directed to the load balancer, which forwards the request to either connector as appropriate.

For more information about configuring Directories Management for high availability, see Configure Directories Management for High Availability.

Infrastructure Web Server

The Infrastructure Web server components all support active-active high availability. To enable high availability for these components, place them under a load balancer.

Infrastructure Manager Service

The manager service component supports active-passive high availability. To enable high availability for this component, place two manager services under a load balancer. In vRealize Automation 7.3 and newer, failover is automatic.

If the active manager service fails, stop the Windows service, if it is not already stopped under the load balancer. Enable the passive manager service and restart the Windows service under the load balancer. See Install the Active Manager Service.
Agents
Agents support active-active high availability. For information about configuring agents for high availability, see the vRealize Automation configuration documentation. Check the target service for high availability.

Distributed Execution Manager Worker
A Distributed Execution Manager (DEM) running under the Worker role supports active-active high availability. If a DEM Worker instance fails, the DEM Orchestrator detects the failure and cancels workflows that the DEM Worker instance is running. When the DEM Worker instance comes back online, it detects that the DEM Orchestrator has canceled the workflows of the instance and stops running them. To prevent workflows from being canceled prematurely, leave a DEM Worker instance offline for several minutes before you cancel its workflows.

Distributed Execution Manager Orchestrator
DEMs running under the Orchestrator role support active-active high availability. When a DEM Orchestrator starts, it searches for another running DEM Orchestrator.
- If it finds no DEM Orchestrator instances running, it starts running as the primary DEM Orchestrator.
- If it does find another running DEM Orchestrator, it monitors the other primary DEM Orchestrator to detect an outage.
- If it detects an outage, it takes over as the primary instance.

When the previous primary instance comes online again, it detects that another DEM Orchestrator has taken over its role as primary and monitors for failure of the primary Orchestrator instance.

MSSQL Database Server for Infrastructure Components
vRealize Automation supports SQL AlwaysON groups only with Microsoft SQL Server 2016. When installing SQL Server 2016, the database must be created in 100 mode. If you use an older version of Microsoft SQL Server, use a Failover Cluster instance with shared disks. For more information on configuring SQL AlwaysOn groups with MSDTC, see Microsoft article https://msdn.microsoft.com/en-us/library/ms366279.aspx.

vRealize Orchestrator
An internal highly-available instance of vRealize Orchestrator is supplied as part of the vRealize Automation appliance.

vRealize Business for Cloud High Availability Considerations
Use the VMware vSphere HA feature for the vRealize Business for Cloud Edition appliance.
To configure the VMware vSphere HA feature on the VMware ESXi host, see the vCenter Server and Host Management documentation.
# vRealize Automation Hardware Specifications and Capacity Maximums

Install appropriate components for your configuration and capacity needs on each vRealize Automation server profile in your environment.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Components</th>
<th>Required Hardware Specifications</th>
<th>Recommended Hardware Specifications</th>
</tr>
</thead>
</table>
| vRealize Automation Appliance | vRealize Automation Services, vRealize Orchestrator, vRealize Automation Appliance Database | CPU: 4 vCPU  
RAM: 18 GB (See [vRealize Automation Scalability](https://example.com) for more information.)  
Disk: 140 GB  
Network: 1 GB/s | Same as required hardware specifications. |
| Infrastructure Core Server | Web site, Manager Service, DEM Orchestrator, DEM Worker, Proxy Agent       | CPU: 4 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | Same as required hardware specifications. |
| Infrastructure Web Server  | Web site                                                                   | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s |
| Infrastructure Manager Server | Manager Service, DEM Orchestrator                                         | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s |
| Infrastructure Web/Manager Server | Infrastructure Web/Manager Server                                       | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s |
| Infrastructure DEM Server  | (One or more) DEM Workers                                                  | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s Per DEM Worker | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s Per DEM Worker |
| Infrastructure Agent Server | (One or more) Proxy Agent                                                  | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s |
### Server Role

<table>
<thead>
<tr>
<th>Components</th>
<th>Required Hardware Specifications</th>
<th>Recommended Hardware Specifications</th>
</tr>
</thead>
</table>
| MSSQL Database Server | Infrastructure Database | CPU: 2 vCPU  
RAM: 8 GB  
Disk: 40 GB  
Network: 1 GB/s | CPU: 8 vCPU  
RAM: 16 GB  
Disk: 80 GB  
Network: 1 GB/s |
| vRealize Business for Cloud Appliance | vRealize Business for Cloud Appliance services  
vRealize Business for Cloud Database Server | CPU: 2 vCPU  
RAM: 4 GB  
Disk: 50 GB  
Network: 1 GB/s | Same as required hardware specifications |

### vRealize Automation Recommended Capacity Maximums

The following resource capacity maximum values apply to the vRealize Automation large deployment profile.

#### Table 1.2. vRealize Automation Resource Capacity Maximums

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>100</td>
</tr>
<tr>
<td>vSphere Endpoints</td>
<td>20</td>
</tr>
<tr>
<td>Compute Resources</td>
<td>200</td>
</tr>
<tr>
<td>Managed Machines</td>
<td>75,000</td>
</tr>
<tr>
<td>Peak Concurrent Request</td>
<td></td>
</tr>
<tr>
<td>constant</td>
<td>50</td>
</tr>
<tr>
<td>bursts</td>
<td>250</td>
</tr>
<tr>
<td>Peak requests per hour</td>
<td>400</td>
</tr>
<tr>
<td>Business Groups</td>
<td>3000 (with 10 unique users per business group and with no user being a member of more than 50 business groups)</td>
</tr>
<tr>
<td>Reservations</td>
<td>9000 (with 3 reservations per business group)</td>
</tr>
<tr>
<td>Blueprints</td>
<td></td>
</tr>
<tr>
<td>CBP only</td>
<td>6000</td>
</tr>
<tr>
<td>CBP + XaaS</td>
<td>8000</td>
</tr>
<tr>
<td>Catalog Items</td>
<td></td>
</tr>
<tr>
<td>across tenants</td>
<td>4000</td>
</tr>
<tr>
<td>in a single tenant</td>
<td>6000</td>
</tr>
<tr>
<td>User/Group sync with default 18 GB memory</td>
<td></td>
</tr>
<tr>
<td>number of users</td>
<td>95027</td>
</tr>
</tbody>
</table>
Table 1-2. vRealize Automation Resource Capacity Maximums (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of groups</td>
<td>20403 (each group contains 4 users including one level of nesting)</td>
</tr>
<tr>
<td>User/Group with memory increased to 30 GB</td>
<td></td>
</tr>
<tr>
<td>number of users</td>
<td>100,000</td>
</tr>
<tr>
<td>number of groups</td>
<td>750 (each group contains 4000 users and each user is in 30 groups)</td>
</tr>
</tbody>
</table>

**vRealize Automation Small Deployment Requirements**

A vRealize Automation small deployment comprises systems of 10,000 managed machines or fewer and includes the appropriate virtual machines, load balancers, and port configurations. The small deployment serves as a starting point for a vRealize Automation deployment that enables you to scale in a supported manner to a medium or large deployment.

When deploying vRealize Automation, use the Enterprise deployment process to provide a separate infrastructure Web site and Manager Service address.

**Support**

A small deployment can support the following items.

- 10,000 managed machines
- 500 catalog items
- 10 concurrent machine provisions

**Requirements**

A small deployment must be configured with the appropriate components.

- vRealize Automation appliance: vrava-1.ra.local
- Infrastructure Core server: inf-1.ra.local.
- MSSQL Database Server: mssql.ra.local
- vRealize Business for Cloud appliance: vrb.ra.local

**DNS Entries**

<table>
<thead>
<tr>
<th>DNS Entry</th>
<th>Points To</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrava.ra.local</td>
<td>vrava-1.ra.local</td>
</tr>
<tr>
<td>web.ra.local</td>
<td>inf.ra.local</td>
</tr>
<tr>
<td>manager.ra.local</td>
<td>inf.ra.local</td>
</tr>
</tbody>
</table>
## Certificates

The host names used in this table are examples only.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>CN or SAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>SAN contains vra.va.sqa.local and vra.va-1.sqa.local</td>
</tr>
<tr>
<td>Infrastructure Core Server</td>
<td>SAN contains web.ra.local, managers.ra.local and inf-1.ra.local</td>
</tr>
<tr>
<td>vRealize Business for Cloud Server</td>
<td>CN = vrb.ra.local</td>
</tr>
</tbody>
</table>

## Ports

Users require access to certain ports. All ports listed are default ports.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>443, 8444. Port 8444 is required for the Virtual Machine Remote Console. Port 8283 is required for access to the vRealize Orchestrator Control Center.</td>
</tr>
</tbody>
</table>

Administrators require access to certain ports, in addition to the ports that users require.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>5480, 8443. Port 8443 is used for advanced identity management configuration. VMware Identity Manager to Active Directory: 389, 636, 3268, 3269 VMware Identity Manager to Domain Controller: 88, 464, 135</td>
</tr>
<tr>
<td>vRealize Business for Cloud</td>
<td>5480</td>
</tr>
<tr>
<td>Server Role</td>
<td>Inbound Ports</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vRealize Automation appliance</td>
<td>HTTPS: 443</td>
</tr>
<tr>
<td></td>
<td>Adapter Configuration: 8443</td>
</tr>
<tr>
<td></td>
<td>Remote Console Proxy: 8444</td>
</tr>
<tr>
<td></td>
<td>SSH: 22</td>
</tr>
<tr>
<td></td>
<td>Virtual Appliance Management Console: 5480</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Infrastructure Core Server          | HTTPS: 443                      | vRealize Automation virtual appliance: 443, 5480                                             |
|                                    | MSDTC: 135, 1024 - 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment. | vSphere Endpoint: 443                                                                            |
|                                    | vSphere Endpoint: 443            | Infrastructure Core requires access to vSphere Endpoint Port 443 to obtain a ticket for VMware Remote Console. |
|                                    |                                 | The vRealize Automation appliance requires access to ESXi host port 902 to proxy traffic to the consumer. |
|                                    |                                 | MSSQL: 135, 1433, 1024 - 65535                                                                |
|                                    |                                 | MSDTC: 135, 1024 - 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment. |</p>
<table>
<thead>
<tr>
<th>Server Role</th>
<th>Inbound Ports</th>
<th>Service/System Outbound Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSQL Database Server</td>
<td>MSSQL: 1433</td>
<td>Infrastructure Core Server: 135, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment. MSDTC: 135, 1024 - 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
</tbody>
</table>
| vRealize Business for Cloud Appliance | HTTPS: 443                  | vRealize Automation virtual appliance:443
|                                   | SSH: 22                      | Infrastructure Core:443                                                                        |
|                                   | Virtual Appliance Management Console: 5480 |                                                                                               |
| Global Catalog                    |                              | Global Catalog: 3268, 3269                                                                     |
Minimum Footprints

Figure 1-1. Minimum footprint for small configuration of vRealize Automation

- vRA Virtual Appliance DNS Entry: vrava.ra.local
- vRA Virtual Appliance: vrava-1.ra.local
- Infrastructure Web DNS Entry: web.ra.local
- Infrastructure Web DNS Entry: manager.ra.local
- Infrastructure Core: inf-1.ra.local
- SQL Database Server: Small-mssql.ra.local
- Fabric

**Users**

443, 8444, 8283

Not Shown:
- All Infrastructure systems require access to Port 5480 of all vRealize Appliances for Log Collection (vRA Settings > Cluster > Collect Logs on Virtual Appliance:5480) to function.
- For Virtual Machine Remote Console, vRealize Appliance requires access to VMware ESXi Port 902, and Infrastructure Core Server requires access to vSphere Endpoint Port 443.

*135
1433
*1024 – 65535

*Please see Database Deployment section for information on how to narrow this range

In addition, bi-directional communication is required.
vRealize Automation Medium Deployment Requirements

A vRealize Automation medium deployment comprises systems of 30,000 managed machines or fewer and includes the appropriate virtual machines, load balancers, and port configurations.

Support

A medium deployment can support the following items.

- 30,000 managed machines
- 1000 catalog items
- 50 machine provisions

Requirements

A medium deployment most meet the appropriate system configuration requirements.

Virtual Appliances

- vRealize Automation appliance 1: vrava-1.ra.local
- vRealize Automation appliance 2: vrava-2.ra.local
- vRealize Automation appliance 2: vrava-3.ra.local
- vRealize Business for Cloud appliance: vrb.ra.local

Windows Server Virtual Machines

- Infrastructure Web/Manager Server 1 (Active Web or DEM-O, Active Manager): inf-1.ra.local
- Infrastructure Web/Manager Server 2 (Active Web or DEM-O, Passive Manager): inf-2.ra.local
- Infrastructure DEM Server 1: dem-1.ra.local
- Infrastructure DEM Server 2: dem-2.ra.local
- Infrastructure Agent Server 1: agent-1.ra.local
- Infrastructure Agent Server 2: agent-2.ra.local

Database Servers
- MSSQL Failover Cluster Instance: mssql.ra.local

Load Balancers
- vRealize Automation appliance load balancer: med-vrava.ra.local
- Infrastructure Web load balancer: med-web.ra.local
- Infrastructure Manager Service load balancer: med-manager.ra.local

Certificates
The host names that are used in this table are examples only.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>CN or SAN</th>
</tr>
</thead>
</table>
| vRealize Automation appliance | SAN contains the following host names:  
- vrava.ra.local  
- vrava-1.ra.local  
- vrava-2.ra.local |
| Infrastructure Web or Manager server | SAN contains the following host names:  
- web.ra.local  
- manager.ra.local  
- inf-1.ra.local  
- inf-2.ra.local |
| vRealize Business for Cloud appliance | CN = vrb.ra.local |

Ports
Users require access to certain ports. All ports listed are default ports.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Port</th>
</tr>
</thead>
</table>

Administrators require access to certain ports, in addition to the ports that users require.
<table>
<thead>
<tr>
<th>Server Role</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance management interface</td>
<td>5480, 8443. Port 8443 is for advanced identity management configuration. VMware Identity Manager to Active Directory: 389, 636, 3268, 3269 VMware Identity Manager to Domain Controller: 88, 464, 135</td>
</tr>
<tr>
<td>vRealize Appliance Orchestrator Control Center</td>
<td>8283</td>
</tr>
<tr>
<td>vRealize Business for Cloud Server</td>
<td>5480</td>
</tr>
</tbody>
</table>

The following table shows inter-application communication.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Inbound Ports</th>
<th>Outbound Ports for Service or System</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>HTTPS:</td>
<td>LDAP:389 vRealize Automationappliance (All other): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 vRealize Automation Infrastructure Web load balancer: 443 VMware ESXi: 902. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. Kerberos Authentication: 88 Computer Object Password renewal: 464</td>
</tr>
<tr>
<td></td>
<td>Adapter Configuration: 8443</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>Remote Console Proxy: 8444</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>Postgres: 5432</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>RabbitMQ: 4369, 25672, 5671, 5672</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>ElasticSearch: 9300, 40002, 40003</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>Stomp: 61613 SSH: 22</td>
<td>vRealize Automation appliance load balancer: 443 vRealize Automation Infrastructure Web load balancer: 443 vRealize Automation appliance: 5480. vSphere Endpoint: 443. Infrastructure Web or Manager requires access to vSphere Endpoint port 443 to obtain a ticket for Virtual Machine Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user. MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.</td>
</tr>
</tbody>
</table>

Infrastructure Web/Manager Server

HTTPS: 443
MSDTC: 135, 1024-65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment.
<table>
<thead>
<tr>
<th>Server Role</th>
<th>Inbound Ports</th>
<th>Outbound Ports for Service or System</th>
</tr>
</thead>
</table>
| Infrastructure DEM Server| NA            | vRealize Automation appliance load balancer: 443  
vRealize Automation Infrastructure Web load balancer: 443  
vRealize Automation Infrastructure Manager load balancer: 443  
vRealize Automation appliance: 5480. |
| Infrastructure Agent Server| NA            | vRealize Automation Infrastructure Web load balancer: 443  
vRealize Automation Infrastructure Manager load balancer: 443  
vRealize Automation appliance: 5480. |
| MSSQL Database Server    | MSSQL: 1433  
MSDTC: 135, 1024 - 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment. | Infrastructure Web/Manager Server: 135, 1024 - 65535. For information about how to narrow this range, see the Database Deployment section of vRealize Automation Deployment. |
| vRealize Business for Cloud Server | HTTPS: 443  
SSH: 22  
vRealize Automation appliance management interface: 5480 | vRealize Automation appliance load balancer: 443  
vRealize Automation Infrastructure Web load balancer: 443 |
| Global Catalog           |               | Global Catalog: 3268, 3269 |

Load balancers require access through the following ports.

<table>
<thead>
<tr>
<th>Load Balancer</th>
<th>Ports Balanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance load balancer</td>
<td>443, 8444</td>
</tr>
<tr>
<td>vRealize Automation Infrastructure Web load balancer</td>
<td>443</td>
</tr>
<tr>
<td>vRealize Automation Infrastructure Manager Service load balancer</td>
<td>443</td>
</tr>
</tbody>
</table>
Figure 1-3. Minimum footprint for vRealize Automation medium configuration

---

**Graphics**

Not Shown:
All Infrastructure systems require access to Port 5480 of all vRealize Appliances for Log Collection (vRA > Cluster > Collect Logs on Virtual Appliance:5480) to function.

For Virtual Machine Remote Console, vRealize Appliance requires access to VMware ESXi Port 902, and Infrastructure Core Server requires access to vSphere Endpoint Port 443.

---

*Please see Database Deployment section for information on how to narrow this range

In addition, bi-directional communication is required.
vRealize Automation Large Deployment Requirements

A vRealize Automation large deployment comprises systems of 75,000 managed machines or fewer and includes the appropriate virtual machines, load balancers, and port configurations.

Support

A large deployment can support the following items.

- 75,000 managed machines
- 2500 catalog items
- 100 concurrent machine provisions

Requirements

A large deployment must meet the appropriate system configuration requirements.

Virtual Appliances

- vRealize Automation appliance 1: vrava-1.ra.local
- vRealize Automation appliance 2: vrava-2.ra.local
- vRealize Automation appliance 2: vrava-3.ra.local
- vRealize Business for Cloud appliance: vrb.ra.local

Windows Server Virtual Machines

- Infrastructure Web Server 1: web-1.ra.local
- Infrastructure Web Server 2: web-2.ra.local
- Infrastructure Manager Server 1: manager-1.ra.local
- Infrastructure Manager Server 2: manager-2.ra.local
- Infrastructure DEM Server 1: dem-1.ra.local
- Infrastructure DEM Server 2: dem-2.ra.local
- Infrastructure Agent Server 1: agent-1.ra.local
- Infrastructure Agent Server 2: agent-2.ra.local
- Clustered MSSQL Database: mssql.ra.local

Load Balancers
- vRealize Automation appliance load balancer: vrava.ra.local
- Infrastructure Web load balancer: web.ra.local
- Infrastructure manager service load balancer: manager.ra.local

Certificates
The host names used in this table are examples only.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>CN or SAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance</td>
<td>SAN contains the following host names:</td>
</tr>
<tr>
<td></td>
<td>■ vrava.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ vrava-1.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ vrava-2.ra.local</td>
</tr>
<tr>
<td>Infrastructure Web server</td>
<td>SAN contains the following host names:</td>
</tr>
<tr>
<td></td>
<td>■ web.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ web-1.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ web-2.ra.local</td>
</tr>
<tr>
<td>Infrastructure manager server</td>
<td>SAN contains the following host names:</td>
</tr>
<tr>
<td></td>
<td>■ manager.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ manager-1.ra.local</td>
</tr>
<tr>
<td></td>
<td>■ manager-2.ra.local</td>
</tr>
<tr>
<td>vRealize Business for Cloud appliance</td>
<td>CN = vrb.ra.local</td>
</tr>
</tbody>
</table>

Ports
Users require access to certain ports. All ports listed are default ports.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance load balancer</td>
<td>443, 8444, 8283 Port 8444 is required for the VMware Remote Console Port 8382 is required for vRealize Orchestrator Control Center.</td>
</tr>
</tbody>
</table>

Administrators require access to certain ports, in addition to the ports that users require.
Server Role | Port
--- | ---
vRealize Automation appliance | 5480, 8283, 8443. Port 8443 is used for advanced identity management configuration.
VMware Identity Manager to Active Directory: 389, 636, 3268, 3269
VMware Identity Manager to Domain Controller: 88, 464, 135

vRealize Business for Cloud server | 5480

The system must support the appropriate inter-application communication.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Inbound Ports</th>
<th>Outbound Ports for Service or System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Web server</td>
<td>HTTPS: 443, MSDTC: 443, 1024-65535, For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment</td>
<td>vRealize Automation appliance load balancer: 443, vRealize Automation appliance virtual appliance: 5480, vSphere endpoint: 443, Infrastructure Web requires access to vSphere endpoint port 443 to obtain a ticket for VMware Remote Console. The vRealize Automation appliance requires access to ESXi host port 902 to proxy console data to the user, MSSQL: 135, 1433, 1024 to 65535, For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment</td>
</tr>
<tr>
<td>Server Role</td>
<td>Inbound Ports</td>
<td>Outbound Ports for Service or System</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Infrastructure manager server</td>
<td>HTTPS: 443</td>
<td>vRealize Automation appliance load balancer: 443</td>
</tr>
<tr>
<td></td>
<td>MSDTC: 135, 1024-65535</td>
<td>vRealize Automation Infrastructure Web Load Balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation appliance: 443, 5480</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSSQL: 135, 1433, 1024 to 65535. For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td>Infrastructure DEM server</td>
<td>NA</td>
<td>vRealize Automation appliance load balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation Infrastructure Web load Balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation infrastructure manager load balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Orchestrator load balancer: 8281</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation appliance: 5480.</td>
</tr>
<tr>
<td>Infrastructure agent server</td>
<td>NA</td>
<td>vRealize Automation infrastructure Web load balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation infrastructure manager load balancer: 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vRealize Automation appliance: 5480.</td>
</tr>
<tr>
<td>MSSQL database server</td>
<td>MSSQL: 1433</td>
<td>Infrastructure Web server: 135, 1024-65535. For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td>MSDTC: 135, 1024-65535</td>
<td>Infrastructure manager server: 135, 1024-65535. For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information about how to narrow this range, see the database deployment section of vRealize Automation Deployment.</td>
</tr>
<tr>
<td>vRealize Business for Cloud server</td>
<td>HTTPS: 443</td>
<td>vRealize Automation appliance load balancer: 443</td>
</tr>
<tr>
<td></td>
<td>SSH: 22</td>
<td>vRealize Automation Infrastructure Web load balancer: 443</td>
</tr>
<tr>
<td></td>
<td>vRealize Automation appliance management interface: 5480</td>
<td></td>
</tr>
<tr>
<td>Global Catalog</td>
<td></td>
<td>Global Catalog: 3268, 3269</td>
</tr>
</tbody>
</table>

Load balancers require access through the following ports.
<table>
<thead>
<tr>
<th>Load Balancer</th>
<th>Ports Balanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation appliance load balancer</td>
<td>443, 8444</td>
</tr>
<tr>
<td>vRealize Automation infrastructure Web load balancer</td>
<td>443</td>
</tr>
<tr>
<td>vRealize Automation manager server load balancer</td>
<td>443</td>
</tr>
</tbody>
</table>
Installing and Upgrading vRealize Automation

Graphics

Figure 1-5. Minimum footprint for vRealize Automation large configuration

All Infrastructure systems require access to Port 5480 of all vRealize Appliances for Log Collection (vRA > Cluster > Collect Logs on Virtual Appliance:5480) to function. For Virtual Machine Remote Console, vRealize Appliance requires access to VMware ESXi Port 902, and Infrastructure Core Server requires access to vSphere Endpoint Port 443. Virtual Appliances must be able to access the Active Directories which are configured as Directories for Authentication.

*Please see Database Deployment section for information on how to narrow this range

**Endpoint communication ports vary by endpoint design and configuration

**Varies

*135
1433
*1024 – 65535

vRA Virtual Appliance LoadBalancer (Port 443, 8444, 8283)
vrava.ra.local

vRA Virtual Appliance 1
vrava-1.ra.local

vRA Virtual Appliance 2
vrava-2.ra.local

vRA Virtual Appliance 3
vrava-3.ra.local

vRA Infrastructure Web Load Balancer [Port 443]
web.ra.local

vRA Infrastructure Web Server 1
web-1.ra.local

vRA Infrastructure Web Server 2
web-2.ra.local

vRA Infrastructure Manager Load Balancer [Port 443]
manager.ra.local

vRA Infrastructure Manager Service 1
manager-1.ra.local

vRA Infrastructure Manager Service 2
manager-2.ra.local

vRA Infrastructure Proxy Agent 1
agent-1.ra.local

vRA Infrastructure Proxy Agent 2
agent-2.ra.local

vRA Infrastructure DEM Server 1
dem-1.ra.local

vRA Infrastructure DEM Server 2
dem-2.ra.local

Fabric

Clumped MSSQL Database
mssql.ra.local

Users

443, 8444, 8283

Ports Required for Appliances to Replicate/Communicate 4369, 5432, 5671, 5672, 9300, 25672, 4002, 40003

NOT SHOWN

**Endpoint communication ports vary by endpoint design and configuration

VMaddition: bi-directional communication is required.
vRealize Automation Multi-Data Center Data Deployments

vRealize Automation supports managing resources in remote data centers.

To manage vSphere, HyperV, or Xen resources in remote data centers, deploy the proxy agent on a virtual machine in the remote data center.

**Note** The diagram below shows a vSphere deployment. Other endpoints require no additional configuration.

Because vRealize Orchestrator workflows will potentially communicate over a WAN, observe best practices as stated in the *vRealize Orchestrator Coding Design Guide*.

### Table 1-3. Required Ports for WAN Communication

<table>
<thead>
<tr>
<th>Role</th>
<th>Inbound Ports</th>
<th>Service/System Outbound Ports</th>
</tr>
</thead>
</table>
| vRealize Automation appliance - including embedded vRealize Orchestrator | N/A | vSphere endpoint: 443
| | | ESIXi Hosts: 902 |
| vRealize Automation Infrastructure Load Balancer | vRealize Automation Infrastructure Proxy Agent: 443 | N/A |
| vRealize Automation Infrastructure Web Server | N/A | vSphere endpoint: 443 |
| vRealize Automation Infrastructure Manager Load Balancer | vRealize Automation Infrastructure Proxy Agent: 443 | N/A |
| vRealize Automation Infrastructure DEM-worker Servers | N/A | Endpoint: **varies** |

* If DEM-workers are installed on the Manager Service machine or another server, these ports must be open between that machine and the target endpoint.
** The port required to communicate with an external endpoint varies depending on the endpoint. By default for vSphere, this is port 443.

**Figure 1-7. vRealize Automation Multi-Site Configuration**

**vRealize Automation Secure Configuration**

Secure Configuration describes how to verify, configure, and update the security profile of a vRealize Automation deployment according to VMware guidelines.

Secure configuration covers the following topics:

- Software Infrastructure security
- Deployed Configuration security
- Host Network security

**vRealize Automation Secure Baseline Overview**

VMware provides comprehensive recommendations to help you verify and configure a secure baseline for your vRealize Automation system.
Use the appropriate tools and procedures as specified by VMware to verify and maintain a secure, hardened baseline configuration for your vRealize Automation system. Some vRealize Automation components are installed in a hardened or partially-hardened state, but you should review and verify configuration of each component in light of VMware security recommendations, company security policies, and known threats.

**vRealize Automation Security Posture**

The security posture of vRealize Automation assumes a holistically secure environment based on system and network configuration, organizational security policies, and security best practices.

When verifying and configuring hardening of a vRealize Automation system, consider each of the following areas as addressed by VMware hardening recommendations.

- Secure Deployment
- Secure Configuration
- Network Security

To ensure that your system is securely hardened, consider VMware recommendations and your local security policies as they relate to each of these conceptual areas.

**System Components**

When considering hardening and the secure configuration of your vRealize Automation system, ensure that you understand all components and how they work together to support system functionality.

Consider the following components when planning and implementing a secure system.

- vRealize Automation appliance
- IaaS Component

To familiarize yourself with vRealize Automation and how the components operate together, see Foundations and Concepts in the VMware vRealize Automation documentation center. For information about typical vRealize Automation deployments and architecture, see vRealize Automation Reference Architecture.

**Verifying the Integrity of Installation Media**

Users should always verify the integrity of the installation media before installing a VMware product.

Always verify the SHA1 hash after you download an ISO, offline bundle, or patch to ensure integrity and authenticity of the downloaded files. If you obtain physical media from VMware and the security seal is broken, return the software to VMware for a replacement.

After you download the media, use the MD5/SHA1 sum value to verify the integrity of the download. Compare the MD5/SHA1 hash output with the value posted on the VMware Web site. SHA1 or MD5 hash should match.

For more information about verifying the integrity of the installation media, see http://kb.vmware.com/kb/1537.
Hardening VMware System Software Infrastructure

As part of your hardening process, assess the deployed software infrastructure that supports your VMware system and verify that it meets VMware hardening guidelines.

Before hardening your VMware system, review and address security deficiencies in your supporting software infrastructure to create a completely hardened and secure environment. Software infrastructure elements to consider include operating system components, supporting software, and database software. Address security concerns in these and other components according to the manufacturer's recommendations and other relevant security protocols.

Hardening the VMware vSphere® Environment

Assess the VMware vSphere® environment and verify that the appropriate level of vSphere hardening guidance is enforced and maintained.

For more guidance about hardening, see http://www.vmware.com/security/hardening-guides.html.

As part of a comprehensively hardened environment, VMware vSphere® infrastructure must meet security guidelines as defined by VMware.

Hardening the Infrastructure as a Service Host

Verify that your Infrastructure as a Service Microsoft Windows host machine is hardened according to VMware guidelines.

Review the recommendations in the appropriate Microsoft Windows hardening and secure best practice guidelines, and ensure that your Windows Server host is appropriately hardened. Not following the hardening recommendations might result in exposure to known security vulnerabilities from insecure components on Windows releases.

To verify that your version is supported, see the vRealize Automation Support Matrix.

Contact your Microsoft vendor about the correct guidance for hardening practices of Microsoft products.

Hardening Microsoft SQL Server

Verify that the Microsoft SQL Server database meets security guidelines as established by Microsoft and VMware.

Review the recommendations in the appropriate Microsoft SQL Server hardening and secure best practice guidelines. Review all Microsoft security bulletins regarding the installed version of Microsoft SQL Server. Not following the hardening recommendations might result in exposure to known security vulnerabilities from insecure components on Microsoft SQL Server versions.

To verify that your version Microsoft SQL Server is supported, see the vRealize Automation Support Matrix.

Contact your Microsoft vendor for guidance about hardening practices for Microsoft products.
Hardening Microsoft .NET
As part of a comprehensively hardened environment, Microsoft .NET must meet security guidelines as laid out by Microsoft and VMware.

Review the recommendations set out in the appropriate .NET hardening and secure best practice guidelines. Also, review all Microsoft security bulletins regarding the version of Microsoft SQL Server you are using. Failure to follow the hardening recommendations might result in exposure to known security vulnerabilities from insecure Microsoft.NET components.

To verify that your version of Microsoft.NET is supported, see the vRealize Automation Support Matrix. Contact your Microsoft vendor for guidance on hardening practices for Microsoft products.

Hardening Microsoft Internet Information Services (IIS)
Verify that your Microsoft Internet Information Services (IIS) meet all Microsoft and VMware security guidelines.

Review the recommendations set out in the appropriate Microsoft IIS hardening and secure best practice guidelines. Also, review all Microsoft security bulletins regarding the version of IIS you are using. Not following the hardening recommendations might result in exposure to known security vulnerabilities.

To verify that your version is supported, see the vRealize Automation Support Matrix.
Contact your Microsoft vendor for guidance on hardening practices for Microsoft products.

Reviewing Installed Software
Because vulnerabilities in third party and unused software increase the risk of unauthorized system access and disruption of availability, it is important to review all software installed on VMware host machines and evaluate its use.

Do not install software that is not required for the secure operation of the system on the VMware host machines. Uninstall unused or extraneous software.

Inventory Installed Unsupported Software
Assess your VMware deployment and inventory of installed products to verify that no extraneous unsupported software is installed.

For more information about the support policies for third-party products, see the VMware support article at https://www.vmware.com/support/policies/thirdparty.html.

Verify Third-Party Software
VMware does not support or recommend installation of third party software that has not been tested and verified. Insecure, unpatched, or unauthenticated third-party software installed on VMware host machines might put the system at risk of unauthorized access and disruption of availability. If you must use unsupported third-party software, consult the third-party vendor for secure configuration and patching requirements.
VMware Security Advisories and Patches

To maintain maximum security for your system, follow VMware security advisories and apply all relevant patches.

VMware releases security advisories for products. Monitor these advisories to ensure that your product is protected against known threats.

Assess the vRealize Automation installation, patching, and upgrade history and verify that the released VMware Security Advisories are followed and enforced.

For more information about the current VMware security advisories, see http://www.vmware.com/security/advisories/.

Secure Configuration

Verify and update security settings for vRealize Automation virtual appliances and the Infrastructure as a Service component as appropriate for your system configuration. In addition, verify and update configuration of other components and applications.

Securely configuring a vRealize Automation installation involves addressing the configuration of each component individually and as they work together. Consider the configuration of all systems components in concert to achieve a reasonably secure baseline.

Securing the vRealize Automation Appliance

Verify and update security settings for the vRealize Automation appliance as necessary for your system configuration.

Configure security settings for your virtual appliances and their host operating systems. In addition, set or verify configuration of other related components and applications. In some cases, you need to verify existing settings, while in others you must change or add settings to achieve an appropriate configuration.

Change the Root Password

You can change the root password for the vRealize Automation appliance to meet applicable security requirements.

Change the root password on the vRealize Automation appliance using the Virtual Appliance Management Interface. Verify that the root password meets your organization’s corporate password complexity requirements.

Procedure

1. Open the Virtual Appliance Management Interface for your vRealize Automation appliance.  
   https://vRealizeAppliance-url:5480
2. Select the Admin tab on the Virtual Appliance Management Interface.
3. Select the Admin submenu.
4. Enter the existing password in the Current administrator password text box.
5. Enter the new password in the **New administrator password** text box.

6. Enter the new password in the **Retype new administrator password** text box.

7. Click **Save Settings** to save your changes.

**Verify Root Password Hash and Complexity**

Verify that the root password meets your organization’s corporate password complexity requirements.

Validating the root password complexity is required as the root user bypasses the pam_cracklib module password complexity check that is applied to user accounts.

The account password must start with `$6$`, which indicates a sha512 hash. This is the standard hash for all hardened appliances.

**Procedure**

1. To verify the hash of the root password, log in as root and run the `# more /etc/shadow` command.
   
   The hash information is displayed.

   **Figure 1-8. Password Hash Results**

   ![Password Hash Results](image)

   2. If the root password does not contain a sha512 hash, run the `passwd` command to change it.

   All hardened appliances enable `enforce_for_root` for the `pw_history` module, found in the `/etc/pam.d/common-password` file. The system remembers the last five passwords by default. Old passwords are stored for each user in the `/etc/securetty/passwd` file.

**Verify Root Password History**

Verify that the password history is enforced for the root account.

All hardened appliances enable `enforce_for_root` for the `pw_history` module, found in the `/etc/pam.d/common-password` file. The system remembers the last five passwords by default. Old passwords are stored for each user in the `/etc/securetty/passwd` file.

**Procedure**

1. Run the following command:

   `cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so`
2 Ensure that enforce_for_root appears in the returned results.

password required pam_pwhistory.so enforce_for_root remember=5 retry=3

**Manage Password Expiry**

Configure all account password expirations in accordance with your organization's security policies.

By default, all hardened VMware virtual appliance accounts use a 60-day password expiration. On most hardened appliances, the root account is set to a 365-day password expiration. As a best practice, verify that the expiration on all accounts meets both security and operation requirements standards.

If the root password expires, you cannot reinstate it. You must implement site-specific policies to prevent administrative and root passwords from expiring.

**Procedure**

1. Log in to your virtual appliance machines as root and run the following command to verify the password expiration on all accounts.

   ```bash
   # cat /etc/shadow
   ```

   The password expiration is the fifth field (fields are separated by colons) of the shadow file. The root expiration is set in days.

   **Figure 1-9. Password Expiry Field**

2. To modify the expiry of the root account, run a command of the following form.

   ```bash
   # passwd -x 365 root
   ```

   In this command, 365 specifies the number of days until password expiry. Use the same command to modify any user, substituting the specific account for 'root', and replacing the number of days to meet the expiry standards of the organization.

**Managing Secure Shell and Administrative Accounts**

For remote connections, all hardened appliances include the Secure Shell (SSH) protocol. Use SSH only when necessary and manage it appropriately to preserve system security.
SSH is an interactive command-line environment that supports remote connections to VMware virtual appliances. By default, SSH access requires high-privileged user account credentials. Root user SSH activities generally bypass the role-based access control (RBAC) and audit controls of the virtual appliances.

As a best practice, disable SSH in a production environment, and activate it only to troubleshoot problems that you cannot resolve by other means. Leave it enabled only while needed for a specific purpose and in accordance with your organization's security policies. SSH is disabled by default on the vRealize Automation appliance. Depending on your vSphere configuration, you might enable or disable SSH when you deploy your Open Virtualization Format (OVF) template.

As a simple test to determine whether SSH is enabled on a machine, try opening a connection by using SSH. If the connection opens and requests credentials, then SSH is enabled and available for connections.

Secure Shell root User Account

Because VMware appliances do not include pre-configured user accounts, the root account can use SSH to directly log in by default. Disable SSH as root as soon as possible.

To meet the compliance standards for non repudiation, the SSH server on all hardened appliances is pre-configured with the AllowGroups wheel entry to restrict SSH access to the secondary group wheel. For separation of duties, you can modify the AllowGroups wheel entry in the `/etc/ssh/sshd_config` file to use another group such as sshd.

The wheel group is enabled with the `pam_wheel` module for superuser access, so members of the wheel group can su-root, where the root password is required. Group separation enables users to SSH to the appliance, but not to su to root. Do not remove or modify other entries in the AllowGroups field, which ensures proper appliance functionality. After making a change, you must restart the SSH daemon by running the command: 
`
# service sshd restart
`

Enable or Disable Secure Shell on the vRealize Automation Appliances

Enable Secure Shell (SSH) on the vRealize Automation appliance only for troubleshooting. Disable SSH on these components during normal production operation.

You can enable or disable SSH on the vRealize Automation appliance using the Virtual Appliance Management console.

Procedure

1. Navigate to the Virtual Appliance Management Console (VAMI) for your vRealize Automation appliance.
   
   : https://vRealizeAppliance url:5480

2. Click the Admin tab.

3. Click the Admin sub-menu.

4. Select the SSH service enable check box to enable SSH or deselect it to disable SSH.

5. Click Save Settings to save your changes.
Create Local Administrator Account for Secure Shell

As a security best practice, create and configure local administrative accounts for Secure Shell (SSH) on your virtual appliance host machines. Also, remove root SSH access after you create the appropriate accounts.

Create local administrative accounts for SSH, or members of the secondary wheel group, or both. Before you disable direct root access, test that authorized administrators can access SSH by using AllowGroups, and that they can su to root using the wheel group.

Procedure

1. Log in to the virtual appliance as root and run the following commands with the appropriate username.

   ```bash
   # useradd -g users <username> -G wheel -m -d /home/username
   # passwd username
   ```

   Wheel is the group specified in AllowGroups for ssh access. To add multiple secondary groups, use `-G wheel,sshd`.

2. Switch to the user and provide a new password to enforce password complexity checking.

   ```bash
   # su -username
   # username@hostname:~> passwd
   ```

   If the password complexity is met, the password updates. If the password complexity is not met, the password reverts to the original password, and you must rerun the password command.

3. To remove direct login to SSH, modify the `/etc/ssh/sshd_config` file by replacing `(#)PermitRootLogin yes` with `PermitRootLogin no`.

   Alternatively, you can enable/disable SSH in the Virtual Appliance Management Interface (VAMI) by selecting or deselecting the **Administrator SSH login enabled** check box on the **Admin** tab.

What to do next

Disable direct logins as root. By default, the hardened appliances allow direct login to root through the console. After you create administrative accounts for non-repudiation and test them for su-root wheel access, disable direct root logins by editing the `/etc/security` file as root and replacing the `tty1` entry with `console`.

1. Open the `/etc/securetty` file in a text editor.

2. Locate `tty1` and replace it with `console`.

3. Save the file and close it.
Harden the Secure Shell Server Configuration

Where possible, all VMware appliances have a default hardened configuration. Users can verify that their configuration is appropriately hardened by examining the server and client service settings in the global options section of the configuration file.

Procedure

1. Open the `/etc/ssh/sshd_config` server configuration file on the VMware appliance, and verify that the settings are correct.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Daemon Protocol</td>
<td>Protocol 2</td>
</tr>
<tr>
<td>CBC Ciphers</td>
<td>aes256-ctr and aes128-ctr</td>
</tr>
<tr>
<td>TCP Forwarding</td>
<td>AllowTCPForwarding no</td>
</tr>
<tr>
<td>Server Gateway Ports</td>
<td>Gateway Ports no</td>
</tr>
<tr>
<td>X11 Forwarding</td>
<td>X11Forwarding no</td>
</tr>
<tr>
<td>SSH Service</td>
<td>Use the AllowGroups field and specify a group permitted access. Add appropriate members to this group.</td>
</tr>
<tr>
<td>GSSAPI Authentication</td>
<td>GSSAPIAuthentication no, if unused</td>
</tr>
<tr>
<td>Keberos Authentication</td>
<td>KeberosAuthentication no, if unused</td>
</tr>
<tr>
<td>Local Variables (AcceptEnv global option)</td>
<td>Set to disabled by commenting out or enabled for LC_* or LANG variables</td>
</tr>
<tr>
<td>Tunnel Configuration</td>
<td>PermitTunnel no</td>
</tr>
<tr>
<td>Network Sessions</td>
<td>MaxSessions 1</td>
</tr>
<tr>
<td>User Concurrent Connections</td>
<td>Set to 1 for root and any other user. The <code>/etc/security/limits.conf</code> file also needs to be configured with the same setting.</td>
</tr>
<tr>
<td>Strict Mode Checking</td>
<td>Strict Modes yes</td>
</tr>
<tr>
<td>Privilege Separation</td>
<td>UsePrivilegeSeparation yes</td>
</tr>
<tr>
<td>rhosts RSA Authentication</td>
<td>RhostsESAAuthentication no</td>
</tr>
<tr>
<td>Compression</td>
<td>Compression delayed or Compression no</td>
</tr>
<tr>
<td>Message Authentication code</td>
<td>MACs hmac-sha1</td>
</tr>
<tr>
<td>User Access Restriction</td>
<td>PermitUserEnvironment no</td>
</tr>
</tbody>
</table>

2. Save your changes and close the file.

Harden the Secure Shell Client Configuration

As part of your system hardening process, verify hardening of the SSH client by examining the SSH client configuration file on virtual appliance host machines to ensure that it is configured according to VMware guidelines.
Procedure

1 Open the SSH client configuration file, /etc/ssh/ssh_config, and verify that settings in the global options section are correct.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Protocol</td>
<td>Protocol 2</td>
</tr>
<tr>
<td>Client Gateway Ports</td>
<td>Gateway Ports no</td>
</tr>
<tr>
<td>GSSAPI Authentication</td>
<td>GSSAPIAuthentication no</td>
</tr>
<tr>
<td>Local Variables (SendEnv global option)</td>
<td>Provide only LC_* or LANG variables</td>
</tr>
<tr>
<td>CBC Ciphers</td>
<td>aes256-ctr and aes128-ctr only</td>
</tr>
<tr>
<td>Message Authentication Codes</td>
<td>Used in the MACs hmac-sha1 entry only</td>
</tr>
</tbody>
</table>

2 Save your changes and close the file.

Verifying Secure Shell Key File Permissions

To minimize the possibility of malicious attacks, maintain critical SSH key file permissions on your virtual appliance host machines.

After configuring or updating your SSH configuration, always verify that the following SSH key file permissions do not change.

- The public host key files located in /etc/ssh/*key.pub are owned by the root user and have permissions set to 0644 (-rw-r--r--).
- The private host key files located in /etc/ssh/*key are owned by the root user and have permissions set to 0600 (-rw------).

Verify SSH Key File Permissions

Verify that SSH permissions are applied to both public and private key files.

Procedure

1 Check the SSH public key files by running the following command: ls -l /etc/ssh/*key.pub

2 Verify that the owner is root, that the group owner is root, and that the files have permissions set to 0644 (-rw-r--r--).

3 Fix any problems by running the following commands.
   chown root /etc/ssh/*key.pub
   chgrp root /etc/ssh/*key.pub
   chmod 644 /etc/ssh/*key.pub

4 Check the SSH private key files by running the following command: ls -l /etc/ssh/*key

5 Fix any problems by running the following commands.
   chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 644 /etc/ssh/*key

Change the Virtual Appliance Management Interface User

You can add and delete users on the Virtual Appliance Management Interface to create the appropriate level of security.

The root user account for the Virtual Appliance Management Interface uses PAM for authentication, so the clipping levels set by PAM also apply. If you have not appropriately isolated the Virtual Appliance Management Interface, a lock out of the system root account could occur if an attacker attempts to brute force the login. In addition, where the root account is considered insufficient to provide non-repudiation by more than one person in your organization, then you might elect to change the admin user for the management interface.

Prerequisites

Procedure

1 Run the following command to create a new user and add it to the Virtual Appliance Management Interface group.
   useradd -G vami,root user
2 Create a password for the user.
   passwd user
3 (Optional) Run the following command to disable root access on the Virtual Appliance Management Interface.
   usermod -R vami root

Note Disabling root access to the Virtual Appliance Management Interface also disables the ability to update the Administrator, or root, password from the Admin tab.

Set Boot Loader Authentication

To provide an appropriate level of security, configure boot loader authentication on your VMware virtual appliances.

If the system’s boot loader requires no authentication, users with system console access can alter the system boot configuration or boot the system into single user or maintenance mode, which can result in denial of service or unauthorized system access. Because boot loader authentication is not set by default on the VMware virtual appliances, you must create a GRUB password to configure it.

Procedure

1 Verify whether a boot password exists by locating the password --md5 <password-hash> line in the /boot/grub/menu.lst file on your virtual appliances.
2. If no password exists, run the `# /usr/sbin/grub-md5-crypt` command on your virtual appliance.
   An MD5 password is generated, and the command supplies the md5 hash output.

3. Append the password to the `menu.lst` file by running the `# password --md5 <hash from grub-md5-crypt>` command.

**Configure NTP**

For critical time sourcing, disable host time synchronization and use the Network Time Protocol (NTP) on the vRealize Automation appliance.

The NTP daemon on vRealize Automation appliance provides synchronized time services. NTP is disabled by default, so you need to configure it manually. If possible, use NTP in production environments to track user actions and to detect potential malicious attacks and intrusions through accurate audit and log keeping. For information about NTP security notices, see the NTP Web site.

The NTP configuration file is located in the `/etc/` folder on each appliance. You can enable the NTP service for the vRealize Automation appliance and add time servers on the Admin tab of the Virtual Appliance Management Interface.

**Procedure**

1. Open the `/etc/ntp.conf` configuration file on your virtual appliance host machine using a text editor.
2. Set the file ownership to `root:root`.
3. Set the permissions to `0640`.
4. To mitigate the risk of a denial-of-service amplification attack on the NTP service, open the `/etc/ntp.conf` file and ensure that the restrict lines appear in the file.

   ```
   restrict default kod nomodify notrap nopeer noquery
   restrict -6 default kod nomodify notrap nopeer noquery
   restrict 127.0.0.1
   restrict -6 ::1
   ```

5. Save any changes and close the files.

**Configuring TLS for vRealize Automation Appliance Data In-transit**

Ensure that your vRealize Automation deployment uses strong TLS protocols to secure transmission channels for vRealize Automation appliance components.

For performance considerations, TLS is not enabled for localhost connections between some application services. Where defense in depth is of concern, enable TLS on all localhost communications.

**Important** If you are terminating TLS on the load balancer, disable insecure protocols such as SSLv2, SSLv3, and TLS 1.0 on all load balancers.

**Enable TLS on Localhost Configuration**

By default some localhost communication does not use TLS. You can enable TLS across all localhost connections to provide enhanced security.
Procedure

1. Connect to the vRealize Automation appliance using SSH.

2. Set permissions for the vcac keystore by running the following commands.

   ```
   usermod -A vco,coredump,pivotal vco
   chown vcac.pivotal /etc/vcac/vcac.keystore
   chmod 640 /etc/vcac/vcac.keystore
   ```

3. Update the HAProxy configuration.

   a. Open the HAProxy configuration file located at `/etc/haproxy/conf.d` and choose the 20-vcac.cfg service.

   b. Locate the lines containing the following string:

   ```
   server local 127.0.0.1...
   ```

   and add the following to the end of such lines: `ssl verify none`

   This section contains other lines like the following:

   ```
   backend-horizon backend-vro
   backend-vra backend-artifactory
   backend-vra-health
   ```

   c. Change the port for backend-horizon from 8080 to 8443.

4. Get the password of keystorePass.

   a. Locate the property `certificate.store.password` in the `/etc/vcac/security.properties` file.

   ```
   For example, certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==
   ```

   b. Decrypt the value using the following command:

   ```
   vcac-config prop-util -d --p VALUE
   ```

   ```
   For example, vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==
   ```

5. Configure the vRealize Automation service.

   a. Open the `/etc/vcac/server.xml` file.

   b. Add the following attribute to the Connector tag, replacing `certificate.store.password` with the certificate store password value found in `/etc/vcac/security.properties`.

   ```
   scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
   keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
   keystorePass="certificate.store.password"
   ```
Configure the vRealize Orchestrator service.

- Open the `/etc/vco/app-server.xml` file
- Add the following attribute to the Connector tag, replacing certificate.store.password with the certificate store password value found in `/etc/vcac/security.properties`.

```xml
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

Restart the vRealize Orchestrator, vRealize Automation, and haproxy services.

```bash
service vcac-server restart
service vco-server restart
service haproxy restart
```

Note: If the vco-server does not restart, reboot the host computer.

Configure the Virtual Appliance Management Interface.

- Open the `/opt/vmware/share/htdocs/service/café-services/services.py` file.
- Change the `conn = httplib.HTTP()` line to `conn = httplib.HTTPS()` to enhance security.

Enable Federal Information Processing Standard (FIPS) 140-2 Compliance

The vRealize Automation appliance now uses the Federal Information Processing Standard (FIPS) 140-2 certified version of OpenSSL for data-in-transit over TLS on all inbound and outbound network traffic.

You can enable or disable FIPS mode in the vRealize Automation appliance management interface. You can also configure FIPS from the command line while logged in as root, using the following commands:

```bash
vcac-vami fips enable
cvac-vami fips disable
cvac-vami fips status
```

When FIPS is enabled, inbound and outbound vRealize Automation appliance network traffic on port 443 uses FIPS 140–2 compliant encryption. Regardless of the FIPS setting, vRealize Automation uses AES–256 to protect secured data stored on the vRealize Automation appliance.

Note: Currently vRealize Automation only partially enables FIPS compliance, because some internal components do not yet use certified cryptographic modules. In cases where certified modules have not yet been implemented, the AES–256 based encryption is used in all cryptographic algorithms.

Note: The following procedure will reboot the physical machine when you alter the configuration.

Procedure

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

   `https:// vrealize-automation-appliance-FQDN:5480`
2 Select **vRA Settings > Host Settings**.

3 Click the button under the Actions heading on the upper right to enable or disable FIPS.

4 Click **Yes** to restart the vRealize Automation appliance

**Verify that SSLv3, TLS 1.0, and TLS 1.1 are Disabled**

As part of your hardening process, ensure that the deployed vRealize Automation appliance uses secure transmission channels.

**Note** You cannot run the join cluster operation after disabling TLS 1.0/1.1 and enabling TLS 1.2

**Prerequisites**

Complete **Enable TLS on Localhost Configuration**.

**Procedure**

1 Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled in the HAProxy https handlers on the vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Review this file</th>
<th>Ensure the following is present</th>
<th>In the appropriate line as shown</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/haproxy/conf.d/20-vcac.cfg</code></td>
<td>no-sslv3 no-tlsv10 no-tls11</td>
<td>bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL!:eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH:AES+RSA+AES:STRENGTH no-sslv3 no-tlsv10 no-tlsv11</td>
</tr>
<tr>
<td><code>/etc/haproxy/conf.d/30-vro-config.cfg</code></td>
<td>no-sslv3 no-tlsv10 no-tls11</td>
<td>bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL!:eNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES+RSA+AES:STRENGTH no-sslv3 no-tlsv10 no-tlsv11</td>
</tr>
</tbody>
</table>

2 Restart the service.

```
    service haproxy restart
```

3 Open the `/opt/vmware/etc/lighttpd/lighttpd.conf` file, and verify that the correct disable entries appear.

**Note** There is no directive to disable TLS 1.0 or TLS 1.1 in Lighttpd. The restriction on TLS 1.0 and TLS 1.1 use can be partially mitigated by enforcing OpenSSL to not use cipher suites of TLS 1.0 and TLS 1.1.

```
    ssl.use-sslv2 = "disable"
    ssl.use-sslv3 = "disable"
```
4 Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled for the Console Proxy on the vRealize Automation appliance.
   a Edit the /etc/vcac/security.properties file by adding or modifying the following line:
      consoleproxy.ssl.server.protocols = TLSv1.2
   b Restart the server by running the following command:
      service vcac-server restart

5 Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled for the vCO service.
   a Locate the <Connector> tag in the /etc/vco/app-server/server.xml file and add the following attribute:
      sslEnabledProtocols = "TLSv1.2"
   b Restart the vCO service by running the following command.
      service vco-server restart

6 Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled for the vRealize Automation service.
   a Add the following attributes to the <Connector> tag in the /etc/vcac/server.xml file
      sslEnabledProtocols = "TLSv1.2"
   b Restart the vRealize Automation service by running the following command:
      service vcac-server restart

7 Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled for RabbitMQ.

Open the /etc/rabbitmq/rabbitmq.config file and verify that `{versions, ['tlsv1.2', 'tlsv1.1']}` are present in the ssl and ssl_options sections.
8  Restart the RabbitMQ server.

   # service rabbitmq-server restart

9  Verify that SSLv3, TLS 1.0, and TLS 1.1 are disabled for the vIDM service.

   Open the opt/vmware/horizon/workspace/conf/server.xml file for each instance of the
   connector containing SSLEnabled="true" and ensure that the following line is present.

   sslEnabledProtocols="TLSv1.2"

### Configuring TLS Cipher Suites for vRealize Automation Components

For maximum security, you must configure vRealize Automation components to use strong ciphers.

The encryption cipher negotiated between the server and the browser determines the encryption strength
that is used in a TLS session.

To ensure that only strong ciphers are selected, disable weak ciphers in vRealize Automation
components. Configure the server to support only strong ciphers and to use sufficiently large key sizes.
Also, configure all ciphers in a suitable order.

Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also
disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing
DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing
mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites. Also ensure that cipher suites
using Diffie-Hellman (DHE) key exchange are disabled

### Disable Weak Ciphers in HA Proxy

Review the vRealize Automation appliance HA Proxy Service ciphers against the list of acceptable
cipher and disable all of those considered weak.

Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also
disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing
DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing
mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites.

### Procedure

1  Review the /etc/haproxy/conf.d/20-vcac.cfg file ciphers entry of the bind directive and disable
   any that are considered weak.

   bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH
   +AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AESRSA+AES:@STRENGTH
   no-sslv3 no-tlsv10 no-tlsv11
2 Review the /etc/haproxy/conf.d/30-vro-config.cfg file ciphers entry of the bind directive and disable any that are considered weak.

bind ::::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!
eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES256:ECDH+AES256:RSA+AES256:
no-sslv3 no-tlsv10 no-tlsv11

Disable Weak Ciphers in the vRealize Automation appliance

Review the vRealize Automation appliance Console Proxy Service ciphers against the list of acceptable ciphers and disable all of those considered weak.

Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites.

Procedure

1 Open the /etc/vcac/security.properties file in a text editor.

2 Add a line to the file to disable the unwanted cipher suites.

   Use a variation of the following line:

   ```
   consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
   ```

   For example, to disable the AES 128 and AES 256 cipher suites, add the following line:

   ```
   consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
   TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
   TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
   TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
   ```

3 Restart the server using the following command.

   ```
   service vcac-server restart
   ```

Disable Weak Ciphers in vRealize Automation appliance vCO Service

Review vRealize Automation appliance vCO Service ciphers against the list of acceptable ciphers and disable all of those considered weak.

Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites.

Procedure

1 Locate the <Connector> tag in /etc/vco/app/server/server.xml file.
2 Edit or add the cipher attribute to use the desired cipher suites.

Refer to the following example:

ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"

Disable Weak Ciphers in the vRealize Automation appliance RabbitMQ Service

Review vRealize Automation appliance RabbitMQ Service ciphers against the list of acceptable ciphers and disable all of those that are considered weak.

Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites.

Procedure

1 Evaluate the supported cipher suites by running the # /usr/sbin/rabbitmqctl eval 'ssl:_cipher_suites().' command.

The ciphers returned in the following example represent only the supported ciphers. The RabbitMQ server does not use or advertise these ciphers unless configured to do so in the rabbitmq.config file.

Select supported ciphers that meet the security requirements for your organization.

For example, to allow only ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384, review the /etc/rabbitmq/rabbitmq.config file and add the following line to ssl and ssl_options.

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

Restart the RabbitMQ server using the following command.

```
service rabbitmq-server restart
```

Verifying Security of Data-at-Rest

Verify the security of database users and accounts used with vRealize Automation.

**Postgres User**

The postgres linux user account is tied to the postgres database superuser account role, by default it is a locked account. This is the most secure configuration for this user as it is only accessible from the root user account. Do not unlock this user account.

**Database User Account Roles**

The default postgres user account roles should not be utilised for uses outside of application functionality. In order to support non-default database review or reporting activities, an additional account should be created and password appropriately protected.

Run the following script in the command line:

```
vCAC-vami add-db-user newUsername newPassword
```

This will add a new user and a password provided by the user.

**Note** This script must be ran against the master postgres database in the cases when master-slave HA postgres setup is configured.

**Configure PostgreSQL Client Authentication**

Ensure that local trust authentication, is not configured the vRealize Automation appliance PostgreSQL database. This configuration allows any local user, including the database super user, to connect as any PostgreSQL user without a password.

**Note** The Postgres super user account should remain as local trust.

The md5 authentication method is recommended because it sends encrypted passwords.

The client authentication configuration settings reside in the `/storage/db/pgdata/pg_hba.conf` file.

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all postgres trust
```

Installing and Upgrading vRealize Automation

VMware, Inc.  52
If you edit the `pg_hba.conf` file, you must restart the Postgres server by running the following commands before changes can take effect.

```bash
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configure vRealize Automation Application Resources

Review vRealize Automation application resources and restrict file permissions.

**Procedure**

1. Run the following command to verify that files with SUID and GUID bits set are well-defined.

   ```bash
   find / -path /proc -prune -o -type f -perm +6000 -ls
   ```

   The following list should appear.

   ```bash
   2197357  24 -rwsr-xr-x   1 polkituser root       23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-set-default-helper
   2197354  16 -rwxr-xr-x   1 root            polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-read-auth-helper
   2197353  12 -rwxr-x---   1 root            polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-grant-helper-pam
   2197352  20 -rwxr-xr-x   1 root            polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-grant-helper
   2197351  20 -rwxr-xr-x   1 root            polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-explicit-grant-helper
   2197356  24 -rwxr-xr-x   1 root            polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-revoke-helper
   2188203  460 -rws---x---   1 root               root       465364 Apr 22 22:38 /usr/lib64/ssh/ssh-keysign
   2138858  12 -rwxr-xr-x   1 root              tty         10680 May 10  2010 /usr/sbin/utempter
   2142482  144 -rwxr-xr-x   1 root             root       142890 Sep 15  2015 /usr/bin/passwd
   2142477  164 -rwxr-xr-x   1 root             shadow     161782 Sep 15  2015 /usr/bin/chage
   ```
<table>
<thead>
<tr>
<th>Owner</th>
<th>Permissions</th>
<th>Size (Bytes)</th>
<th>Date</th>
<th>Command Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>152850</td>
<td>Sep 15</td>
<td>/usr/bin/chfn</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>365787</td>
<td>Jul 22</td>
<td>/usr/bin/sudo</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>57776</td>
<td>Sep 15</td>
<td>/usr/bin/newgrp</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>40432</td>
<td>Mar 18</td>
<td>/usr/bin/crontab</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>146459</td>
<td>Sep 15</td>
<td>/usr/bin/chsh</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>152387</td>
<td>Sep 15</td>
<td>/usr/bin/gpasswd</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>46967</td>
<td>Sep 15</td>
<td>/usr/bin/expiry</td>
</tr>
<tr>
<td>messagebus</td>
<td>rwsr-x----</td>
<td>47912</td>
<td>Sep 16</td>
<td>/lib64/dbus-1/dbus-daemon-launch-helper</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>35688</td>
<td>Apr 10</td>
<td>/sbin/unix_chkpwd</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>10736</td>
<td>Dec 16</td>
<td>/sbin/unix2_chkpwd</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>63376</td>
<td>May 27</td>
<td>/opt/likewise/bin/ksu</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>40016</td>
<td>Apr 16</td>
<td>/bin/su</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>40048</td>
<td>Apr 15</td>
<td>/bin/ping</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>94808</td>
<td>Mar 11</td>
<td>/bin/mount</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>69240</td>
<td>Mar 11</td>
<td>/bin/umount</td>
</tr>
<tr>
<td>root</td>
<td>rwsr-xr-x</td>
<td>35792</td>
<td>Apr 15</td>
<td>/bin/ping6</td>
</tr>
</tbody>
</table>

2. Run the following command to verify that all files on the virtual appliance have an owner.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

3. Review permissions for all files to the virtual appliance to verify that none of them are world writable by running the following command.

```
find / -name "*." -type f -perm -a+w | xargs ls -ldb
```

4. Run the following command to verify that only the vcac user owns the correct files.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

If no results appear, then all correct files are owned only by the vcac user.

5. Verify that the following files are writeable only by the vcac user.

- /etc/vcac/vcac/security.properties
- /etc/vcac/vcac/solution-users.properties
- /etc/vcac/vcac/sso-admin.properties
- /etc/vcac/vcac/vcac.keystore
- /etc/vcac/vcac/vcac.properties
- /var/log/vcac/*
- /var/lib/vcac/*
- /var/cache/vcac/*

Also verify the following files and their sub-directories

- /var/log/vcac/*
- /var/lib/vcac/*
- /var/cache/vcac/*
6 Verify that only the vcac or root user can read the correct files in the following directories and their sub-directories.
   /etc/vcac/*
   /var/log/vcac/*
   /var/lib/vcac/*
   /var/cache/vcac/*

7 Verify that the correct files are owned only by the vco or root user, as shown in in the following directories and their sub-directories.
   /etc/vco/*
   /var/log/vco/*
   /var/lib/vco/*
   /var/cache/vco/*

8 Verify that the correct files are writeable only by the vco or root user, as shown in in the following directories and their sub-directories.
   /etc/vco/*
   /var/log/vco/*
   /var/lib/vco/*
   /var/cache/vco/*

9 Verify that the correct files are readable only by the vco or root user, as shown in in the following directories and their sub-directories.
   /etc/vco/*
   /var/log/vco/*
   /var/lib/vco/*
   /var/cache/vco/*

Customizing Console Proxy Configuration

You can customize the remote console configuration for vRealize Automation to facilitate troubleshooting and organizational practices.

When you install, configure, or maintain vRealize Automation, you can change some settings to enable troubleshooting and debugging of your installation. Catalog and audit each of the changes you make to ensure that applicable components are properly secured according to their required use. Do not proceed to production if you are not sure that your configuration changes are correctly secured.

Customize VMware Remote Console Ticket Expiry

You can customize the validity period for remote console tickets used in establishing VMware Remote Console connections.
When a user makes VMware Remote Console connections, the system creates and returns a one-time credential that establishes a specific connection to a virtual machine. You can set the ticket expiry for a specified time frame in minutes.

**Procedure**

1. Open the `/etc/vcac/security.properties` file in a text editor.
2. Add a line to the file of the form `consoleproxy.ticket.validitySec=30`.
   
   In this line the numerical value specifies the number of minutes before the ticket expires.
3. Save the file and close it.
4. Restart the vcac-server using the command `/etc/init.d/vcac-server restart`.

The ticket expiry value is reset to the specified time frame in minutes.

**Customize Console Proxy Server Port**

You can customize the port on which the VMware Remote Console console proxy listens for messages.

**Procedure**

1. Open the `/etc/vcac/security.properties` file in a text editor.
2. Add a line to the file of the form `consoleproxy.service.port=8445`.
   
   The numerical value specifies the console proxy service port number, in this case 8445.
3. Save the file and close it.
4. Restart the vcac-server using the command `/etc/init.d/vcac-server restart`.

The proxy service port changes to the specified port number.

**Configure X-XSS-Protection Response Header**

Add the X-XSS-Protection response header to the haproxy configuration file.

**Procedure**

1. Open `/etc/haproxy/conf.d/20-vcac.cfg` for editing.
2. Add the following lines in a front end section:
   
   ```
   rspdel X-XSS-Protection:\ 1;\ mode=block
   rspadd X-XSS-Protection:\ 1;\ mode=block
   ```
3. Reload the HAProxy configuration using the following command.
   
   `/etc/init.d/haproxy reload`

**Configure HTTP Strict Transport Security Response Header**

Add the HTTP Strict Transport (HSTS) response header to the HAProxy configuration.
Procedure
1 Open /etc/haproxy/conf.d/20-vcac.cfg for editing.
2 Add the following lines in a front end section:

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```
3 Reload the HAProxy configuration using the following command.

```
/etc/init.d/haproxy reload
```

Configure X-Frame-Options Response Header
The X-Frame-Options response header may appear twice in some cases.
The X-Frame-Options response header may appear twice because the vIDM service adds this header to
the back end as well as to HAProxy. You can prevent it appearing twice with an appropriate configuration.

Procedure
1 Open /etc/haproxy/conf.d/20-vcac.cfg for editing.
2 Locate the following line in the front end section:

```
rspadd X-Frame-Options:\ SAMEORIGIN
```
3 Add the following lines before the line you located in the preceding step:

```
rspdel X-Frame-Options:\ SAMEORIGIN
```
4 Reload the HAProxy configuration using the following command.

```
/etc/init.d/haproxy reload
```

Configuring Server Response Headers
As a security best practice, configure your vRealize Automation system to limit information available to
potential attackers.
To the extent possible, minimize the amount of information that your system shares about its identity and
version. Hackers and malicious actors can use this information to craft targeted attacks against your Web
server or version.

Configure the Lighttpd Server Response Header
As a best practice, create a blank server header for the vRealize Automation appliance lighttpd server.

Procedure
1 Open the /opt/vmware/etc/lighttpd/lighttpd.conf file in a text editor.
2 Add the server.tag = " " to the file.
3 Save your changes and close the file.
4 Restart the lighttpd server by running the `# /opt/vmware/etc/init.d/vami-lighttp restart` command.

Configure the TCServer Response Header for the vRealize Automation Appliance

As a best practice, create a custom blank server header for the TCServer response header used with the vRealize Automation appliance to limit the possibility of a malicious attacker obtaining valuable information.

Procedure

1 Open the `/etc/vco/app-server/server.xml` file in a text editor.
2 In each `<Connector>` element add `server=" "`.
   
   For example: `<Connector protocol="HTTP/1.1" server="" ......... />`
3 Save your changes and close the file.
4 Restart the server using the following command.
   
   `service vco-server restart`

Configure the Internet Information Services Server Response Header

As a best practice, create a custom blank server header for the Internet Information Services (IIS) server used with the Identity Appliance to limit the possibility of malicious attackers obtaining valuable information.

Procedure

1 Open the `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` file in a text editor.
2 Search for `RemoveServerHeader=0` and change it to `RemoveServerHeader=1`.
3 Save your changes and close the file.
4 Restart the server by running the `iisreset` command.

What to do next

Disable the IIS X-Powered By header by removing HTTP Response headers from the list in the IIS Manager Console.

1 Open the IIS Manager console.
2 Open the HTTP Response Header and remove it from the list.
3 Restart the server by running the `iisreset` command.

Set vRealize Automation appliance Session Timeout

Configure the session timeout setting on the vRealize Automation appliance in accordance with your company security policy.
The vRealize Automation appliance default session timeout on user inactivity is 30 minutes. To adjust this time out value to conform to your organization's security policy, edit the web.xml file on your vRealize Automation appliance host machine.

**Procedure**

2. Find `session-config` and set the `session-timeout` value. See the following code sample.

   <!-- 30 minutes session expiration time -->
   <session-config>
     <session-timeout>30</session-timeout>
     <tracking-mode>COOKIE</tracking-mode>
     <cookie-config>
       <path>/</path>
     </cookie-config>
   </session-config>

3. Restart the server by running the following command.

   `service vcac-server restart`

**Managing Nonessential Software**

To minimize security risks, remove or configure nonessential software from your vRealize Automation host machines.

Configure all software that you do not remove in accordance with manufacturer recommendations and security best practices to minimize its potential to create security breaches.

**Secure the USB Mass Storage Handler**

Secure the USB mass storage handler to prevent its use as the USB device handler with the VMware virtual appliance host machines. Potential attackers can exploit this handler to compromise your system.

**Procedure**

1. Open the /etc/modprobe.conf.local file in a text editor.
2. Ensure that the `install usb-storage /bin/true` line appears in the file.
3. Save the file and close it.

**Secure the Bluetooth Protocol Handler**

Secure the Bluetooth Protocol Handler on your virtual appliance host machines to prevent potential attackers from exploiting it.

Binding the Bluetooth protocol to the network stack is unnecessary and can increase the attack surface of the host.

**Procedure**

1. Open the /etc/modprobe.conf.local file in a text editor.
2 Ensure that the following line appears in this file.
   `install bluetooth /bin/true`

3 Save the file and close it.

**Secure the Stream Control Transmission Protocol**

Prevent the Stream Control Transmission Protocol (SCTP) from loading on your system by default. Potential attackers could exploit this protocol to compromise your system.

Configure your system to prevent the Stream Control Transmission Protocol (SCTP) module from loading unless it is absolutely necessary. SCTP is an unused IETF-standardized transport layer protocol. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes could cause the kernel to dynamically load a protocol handler by opening a socket using the protocol.

**Procedure**

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the following line appears in this file.
   `install sctp /bin/true`

3 Save the file and close it.

**Secure the Datagram Congestion Protocol**

As part of your system hardening activities, prevent the Datagram Congestion Protocol (DCCP) from loading on your virtual appliance host machines by default. Potential attackers can exploit this protocol to compromise your system.

Avoid loading the Datagram Congestion Control Protocol (DCCP) module, unless it is absolutely necessary. DCCP is a proposed transport layer protocol, which is not used. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes can cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

**Procedure**

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the DCCP lines appear in the file.
   ```
   install dccp/bin/true
   install dccp_ipv4/bin/true
   install dccp_ipv6/bin/true
   ```

3 Save the file and close it.

**Secure Network Bridging**

Prevent the network bridging module from loading on your system by default. Potential attackers could exploit it to compromise your system.
Configure your system to prevent the network from loading, unless it is absolutely necessary. Potential attackers could exploit it to bypass network partitioning and security.

**Procedure**

1. Run the following command on all VMware virtual appliance host machines.
   
   ```bash
   # rmmod bridge
   ```

2. Open the `/etc/modprobe.conf.local` file in a text editor.

3. Ensure that the following line appears in this file.
   
   ```bash
   install bridge /bin/false
   ```

4. Save the file and close it.

**Secure Reliable Datagram Sockets Protocol**

As part of your system hardening activities, prevent the Reliable Datagram Sockets Protocol (RDS) from loading on your virtual appliance host machines by default. Potential attackers can exploit this protocol to compromise your system.

Binding the Reliable Datagram Sockets (RDS) Protocol to the network stack increases the attack surface of the host. Unprivileged local processes can cause the system to dynamically load a protocol handler by using the protocol to open a socket.

**Procedure**

1. Open the `/etc/modprobe.conf.local` file in a text editor.

2. Ensure that the `install rds /bin/true` line appears in this file.

3. Save the file and close it.

**Secure Transparent Inter-Process Communication Protocol**

As part of your system hardening activities, prevent the Transparent Inter-Process Communication Protocol (TIPC) from loading on your virtual appliance host machines by default. Potential attackers can exploit this protocol to compromise your system.

Binding the Transparent Inter-Process Communications (TIPC) Protocol to the network stack increases the attack surface of the host. Unprivileged local processes can cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

**Procedure**

1. Open the `/etc/modprobe.conf.local` file in a text editor.

2. Ensure that the `install tipc /bin/true` line appears in this file.

3. Save the file and close it.
Secure Internetwork Packet Exchange Protocol

prevent the Internetwork Packet Exchange Protocol (IPX) from loading on your system by default. Potential attackers could exploit this protocol to compromise your system.

Avoid loading the Internetwork Packet Exchange (IPX) Protocol module unless it is absolutely necessary. IPX protocol is an obsolete network-layer protocol. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes could cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1. Open the /etc/modprobe.conf.local file in a text editor.
2. Ensure that the following line appears in this file.
   
   ```
   install ipx /bin/true
   ```

3. Save the file and close it.

Secure Appletalk Protocol

prevent the Appletalk Protocol from loading on your system by default. Potential attackers could exploit this protocol to compromise your system.

Avoid loading the Appletalk Protocol module unless it is absolutely necessary. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes could cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1. Open the /etc/modprobe.conf.local file in a text editor.
2. Ensure that the following line appears in this file.
   
   ```
   install appletalk /bin/true
   ```

3. Save the file and close it.

Secure DECnet Protocol

prevent the DECnet Protocol from loading on your system by default. Potential attackers could exploit this protocol to compromise your system.

Avoid loading the DECnet Protocol module unless it is absolutely necessary. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes could cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1. Open the DECnet Protocol /etc/modprobe.conf.local file in a text editor.
2. Ensure that the following line appears in this file.
   
   ```
   install decnet /bin/true
   ```

3. Save the file and close it.
Secure Firewire Module
Prevent the Firewire module from loading on your system by default. Potential attackers could exploit this protocol to compromise your system.

Avoid loading the Firewire module unless it is absolutely necessary.

Procedure
1. Open the /etc/modprobe.conf.local file in a text editor.
2. Ensure that the following line appears in this file.
   ```
   install ieee1394 /bin/true
   ```
3. Save the file and close it.

Securing the Infrastructure as a Service Component
When you harden your system, secure the vRealize Automation Infrastructure as a Service (IaaS) component and its host machine to prevent potential attackers from exploiting it.

You must configure security setting for the vRealize Automation Infrastructure as a Service (IaaS) component and the host on which it resides. You must set or verify the configuration of other related components and applications. In some cases, you can verify existing settings, in others you must change or add settings for an appropriate configuration.

Disabling Windows Time Service
As a security best practice, use authorized time servers rather than host time synchronization in a vRealize Automation production environment.

In a production environment, disable host time synchronization and use authorized time servers to support accurate tracking of user actions, and identification of potential malicious attacks and intrusion through auditing and logging.

Configuring TLS for Infrastructure as a Service Data-in-Transit
Ensure that your vRealize Automation deployment uses strong TLS protocols to secure transmission channels for Infrastructure as a Service components.

Secure Sockets Layer (SSL) and the more recently developed Transport Layer Security (TLS) are cryptographic protocols that help ensure system security during network communications between different system components. As SSL is an older standard, many of its implements no longer provide adequate security against potential attacks. Serious weaknesses have been identified with earlier SSL protocols, including SSLv2 and SSLv3. These protocols are no longer considered secure.

Depending on your organization’s security policies you may wish to also disable TLS 1.0.

Note When terminating TLS at the load balancer, also disable weak protocols such as SSLv2, SSLv3, as well as TLS 1.0 if required.
Disable SSLv3 in Internet Information Services
As a security best practice, disable SSLv3 in Internet Information Services (IIS) on the Infrastructure as a Service (IaaS) host server machine.

Procedure
1. Run the Windows registry editor as an administrator.
2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` in the registry window.
3. Right-click on Protocols, and select New > Key.
4. Enter SSL 3.0.
5. In the navigation tree, right-click the newly created SSL 3.0 key, and in the pop-up menu select New > Key and enter Client.
6. In the navigation tree, right-click on the newly created SSL 3.0 key, and in the pop-up menu select New > Key and enter Server.
7. In the navigation tree, under SSL 3.0, right-click Client, and select New > DWORD (32-bit) Value and enter DisabledByDefault.
8. In the navigation tree, under SSL 3.0, select Client, and in the right pane, double-click DisabledByDefault and enter 1.
9. In the navigation tree, under SSL 3.0, right-click Server, and select New > DWORD (32-bit) Value and enter Enabled.
10. In the navigation tree, under SSL 3.0, select Server, and in the right pane, double-click the enabled DWORD and enter 0.
11. Restart the Windows Server.

Disable TLS 1.0 for IaaS
To provide maximum security, configure IaaS to use pooling and disable TLS 1.0.

For more information, see the Microsoft knowledge base article [https://support.microsoft.com/en-us/kb/245030](https://support.microsoft.com/en-us/kb/245030).
Procedure

1. Configure IaaS to use pooling instead of web sockets.
   
   a. Update the Manager Services configuration file `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config` by adding the following values in the `<appSettings>` section:

   ```xml
   <add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
   <add key="Extensibility.Client.PollingInterval" value="2000"/>
   <add key="Extensibility.Client.PollingMaxEvents" value="128"/>
   ```

   b. Restart the Manager Service (VMware vCloud Automation Center Service).

2. Verify that TLS 1.0 is disabled on the IaaS server.
   
   a. Run the registry editor as an administrator.

   b. In the registry window, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols`.

   c. Right-click on Protocols and select **New > Key** and then enter **TLS 1.0**.

   d. In the navigation tree, right-click on the TLS 1.0 key that you just created, and in the pop-up menu select **New > Key** and enter **Client**.

   e. In the navigation tree, right-click on the TLS 1.0 key that you just created and in the pop up menu select **New > Key** and enter **Server**.

   f. In the navigation tree, under TLS 1.0, right-click on **Client**, and then click **New > DWORD (32-bit) Value** and enter **DisabledByDefault**.

   g. In the navigation tree, under TLS 1.0, select **Client**, and in the right pane, double-click **DisabledByDefault DWORD** and enter **1**.

   h. In the navigation tree, under TLS 1.0, right-click **Server**, and select **New > DWORD (32-bit) Value** and enter **Enabled**.

   i. In the navigation tree, under TLS 1.0, select **Server**, and in the right pane, double-click **Enabled DWORD** and enter **0**.

   j. Restart the Windows Server.

Configuring TLS Cipher Suites

For maximum security, you must configure vRealize Automation components to use strong ciphers. The encryption cipher negotiated between the server and the browser determines the encryption strength that is used in a TLS session. To ensure that only strong ciphers are selected, disable weak ciphers in vRealize Automation components. Configure the server to support only strong ciphers and to use sufficiently large key sizes. Also, configure all ciphers in a suitable order.
Cipher Suites that are not Acceptable
Disable cipher suites that do not offer authentication such as NULL cipher suites, aNULL, or eNULL. Also disable anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites. Also ensure that cipher suites using Diffie-Hellman (DHE) key exchange are disabled.

Verifying Host Server Security
As a security best practice, verify the security configuration of your Infrastructure as a Service (IaaS) host server machines.

Microsoft supplies several tools to help you verify security on host server machines. Contact your Microsoft vendor for guidance on the most appropriate use of these tools.

Verify Host Server Secure Baseline
Run the Microsoft Baseline Security Analyzer (MBSA) to quickly confirm that your server has the latest updates or hot fixes. You can use the MBSA to install missing security patches from Microsoft to keep your server up-to-date with Microsoft security recommendations.

Download the latest version of the MBSA tool from the Microsoft website.

Verify Host Server Security Configuration
Use the Windows Security Configuration Wizard (SCW) and the Microsoft Security Compliance Manager (SCM) toolkit to verify that the host server is securely configured.

Run the SCW from the administrative tools from your Windows server. This tool can identify the roles of your server and the installed features including networking, Windows firewalls, and registry settings.
Compare the report with the latest hardening guidance from the relevant SCM for your Windows server.
Based on the results, you can fine tune security settings for each feature such as network services, account settings, and Windows firewalls, and apply the settings to your server.

You can find more information about the SCW tool on the Microsoft Technet Web site.

Protecting Application Resources
As a security best practice, ensure that all relevant Infrastructure as a Service files have the appropriate permissions.

Review Infrastructure as a Service files against your Infrastructure as a Service installation. In most cases, subfolders and files for every folder should have the same settings as the folder.

<table>
<thead>
<tr>
<th>Directory or File</th>
<th>Group or Users</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read &amp; Execute</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>\VMware\vCAC\Agents &lt;agent_name&gt; \logs</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Administrator</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Administrators</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Directory or File</td>
<td>Group or Users</td>
<td>Full Control</td>
<td>Modify</td>
<td>Read &amp; Execute</td>
<td>Read</td>
<td>Write</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------</td>
<td>--------------</td>
<td>--------</td>
<td>----------------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>VMware\vCAC\Agents&lt;agent_name&gt;\temp</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Administrators</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Agents\</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Administrators</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Distributed Execution Manager\</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Distributed Execution Manager\</td>
<td>Administrators</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Distributed Execution Manager\DEM\Logs</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Distributed Execution Manager\DEO\Logs</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Management Agent\</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Server\</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware\vCAC\Web API</td>
<td>SYSTEM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Secure the Infrastructure as a Service Host Machine**

As a security best practice, review basic settings on your Infrastructure as a Service (IaaS) host machine to ensure that it conforms to security guidelines.

Secure miscellaneous accounts, applications, ports, and services on the Infrastructure as a Service (IaaS) host machine.

**Verify Server User Account Settings**

Verify that no unnecessary local and domain user accounts and settings exist. Restrict any user account that is not related to the application functions to those required for administration, maintenance, and troubleshooting. Restrict remote access from domain user accounts to the minimum required to maintain the server. Strictly control and audit these accounts.
Delete Unnecessary Applications
Delete all unnecessary applications from the host servers. Unnecessary applications increase the risk of exposure because of their unknown or unpatched vulnerabilities.

Disable Unnecessary Ports and Services
Review the host server's firewall for the list of open ports. Block all ports that are not required for the IaaS component or critical system operation. See Configuring Ports and Protocols. Audit the services running against your host server, and disable those that are not required.

Configuring Host Network Security
To provide maximum protection against known security threats, configure network interface and communication settings on all VMware host machines.

As part of a comprehensive security plan, configure network interface security settings for the VMware virtual appliances and the Infrastructure as a Service components in accordance with established security guidelines.

Configuring Network Settings for VMware Appliances
To ensure that your VMware virtual appliance host machines support only safe and essential communications, review and edit their network communication settings.

Examine the network IP protocol configuration of your VMware host machines, and configure network settings in accordance with security guidelines. Disable all nonessential communication protocols.

Prevent User Control of Network Interfaces
As a security best practice, allow users only the system privileges that they need to do their jobs on VMware appliance host machines.

Permitting user accounts with privileges to manipulate network interfaces can result in bypassing network security mechanisms or denial of service. Restrict the ability to change network interface settings to privileged users.

Procedure
1. Run the following command on each VMware appliance host machine.
   
   # grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*

2. Make sure that each interface is set to NO.

Set TCP Backlog Queue Size
To provide some level of defense against malicious attacks, configure a default TCP backlog queue size on VMware appliance host machines.

Set the TCP backlog queue sizes to an appropriate default size to provide mitigation for TCP denial or service attacks. The recommended default setting is 1280.
Procedure

1. Run the following command on each VMware appliance host machine.
   
   ```bash
   # cat /proc/sys/net/ipv4/tcp_max_syn_backlog
   ```

2. Open the `/etc/sysctl.conf` file in a text editor.

3. Set the default TCP backlog queue size by adding the following entry to the file.
   
   ```
   net.ipv4.tcp_max_syn_backlog=1280
   ```

4. Save your changes and close the file.

Deny ICMPv4 Echoes to Broadcast Address

As a security best practice, verify that your VMware appliance host machines ignore ICMP broadcast address echo requests.

Responses to broadcast Internet Control Message Protocol (ICMP) echoes provide an attack vector for amplification attacks and can facilitate network mapping by malicious agents. Configuring your appliance host machines to ignore ICMPv4 echoes provides protection against such attacks.

Procedure

1. Run the
   
   ```bash
   # cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
   ```
   command on the VMware virtual appliance host machines to confirm that they deny IPv4 broadcast address echo requests.

   If the host machines are configured to deny IPv4 redirects, this command will return a value of 0 for `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

2. To configure a virtual appliance host machine to deny ICMPv4 broadcast address echo requests, open the `/etc/sysctl.conf` file on Windows host machines in a text editor.

3. Locate the entry that reads `net.ipv4.icmp_echo_ignore_broadcasts=0`. If the value for this entry is not set to zero or if the entry does not exist, add it or update the existing entry accordingly.

4. Save the changes and close the file.

Disable IPv4 Proxy ARP

Verify that IPv4 Proxy ARP is disabled if not otherwise required on your VMware appliance host machines to prevent unauthorized information sharing.

IPv4 Proxy ARP allows a system to send responses to ARP requests on one interface on behalf of hosts connected to another interface. Disable it if not needed to prevent leakage of addressing information between the attached network segments.
Procedure

1. Run the `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` command on the VMware virtual appliance host machines to verify that IPv4 Proxy ARP is disabled.

   If IPv6 Proxy ARP is disabled on the host machines, this command will return values of 0.

   ```
   /proc/sys/net/ipv4/conf/all/proxy_arp:0
   /proc/sys/net/ipv4/conf/default/proxy_arp:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2. If you need to configure IPv6 Proxy ARP on host machines, open the `/etc/sysctl.conf` file in a text editor.

3. Check for the following entries.

   ```
   net.ipv4.conf.default.proxy_arp=0
   net.ipv4.conf.all.proxy_arp=0
   ```

   If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4. Save any changes you made and close the file.

Deny IPv4 ICMP Redirect Messages

As a security best practice, verify that your VMware virtual appliance host machines deny IPv4 ICMP redirect messages.

Routers use ICMP redirect messages to tell hosts that a more direct route exists for a destination. A malicious ICMP redirect message can facilitate a man-in-the-middle attack. These messages modify the host's route table and are unauthenticated. Ensure that your system is configured to ignore them if they are not otherwise needed.

Procedure

1. Run the `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` command on the VMware appliance host machines to confirm that they deny IPv4 redirect messages.

   If the host machines are configured to deny IPv4 redirects, this command returns the following:

   ```
   /proc/sys/net/ipv4/conf/all/accept_redirects:0
   /proc/sys/net/ipv4/conf/default/accept_redirects:0
   ```

2. If you need to configure a virtual appliance host machine to deny IPv4 redirect messages, open the `/etc/sysctl.conf` file in a text editor.
3 Check the values of the lines that begin with net.ipv4.conf.

If the values for the following entries are not set to zero or if the entries do not exist, add them to the file or update the existing entries accordingly.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

4 Save the changes you made and close the file.

**Deny IPv6 ICMP Redirect Messages**

As a security best practice, verify that your VMware virtual appliance host machines deny IPv6 ICMP redirect messages.

Routers use ICMP redirect messages to tell hosts that a more direct route exists for a destination. A malicious ICMP redirect message can facilitate a man-in-the-middle attack. These messages modify the host's route table and are unauthenticated. Ensure your system is configured to ignore them if they not otherwise needed.

**Procedure**

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` command on the VMware virtual appliance host machines to confirm that they deny IPv6 redirect messages.

   If the host machines are configured to deny IPv6 redirects, this command returns the following:
   
   `/proc/sys/net/ipv6/conf/all/accept_redirects:0`
   `/proc/sys/net/ipv6/conf/default/accept_redirects:0`

2 To configure a virtual appliance host machine to deny IPv4 redirect messages, open the `/etc/sysctl.conf` file in a text editor.

3 Check the values of the lines that begin with net.ipv6.conf.

   If the values for the following entries in the are not set to zero or if the entries do not exist, add them to the file or update the existing entries accordingly.

   ```
   net.ipv6.conf.all.accept_redirects=0
   net.ipv6.conf.default.accept_redirects=0
   ```

4 Save the changes and close the file.

**Log IPv4 Martian Packets**

As a security best practice, verify that your VMware virtual appliance host machines log IPv4 Martian packets.

Martian packets contain addresses that the system knows to be invalid. Configure your host machines to log these messages so that you can identify misconfigurations or attacks in progress.
Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` command on the VMware appliance host machines to verify that they log IPv4 Martian packets.

If the virtual machines are configured to log Martian packers, they return the following:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/default/log_martians:1
```

If the host machines are configured correctly, no further action is necessary.

2 If you need to configure virtual machines to log IPv4 martian packets, open the `/etc/sysctl.conf` file in a text editor.

3 Check the values of the lines that start with `net.ipv4.conf`.

If the value for the following entries are not set to 1 or if they do not exist, add them to the file or update the existing entries accordingly.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

4 Save your changes and close the file.

Use IPv4 Reverse Path Filtering

As a security best practice, verify that your VMware virtual appliance host machines use IPv4 reverse path filtering.

Reverse-path filtering protects against spoofed source addresses by causing the system to discard packets with source addresses that have no route or a route that does not point towards the originating interface. Configure your host machines to use reverse-path filtering whenever possible. In some cases, depending on the system role, reverse-path filtering can cause the system to discard legitimate traffic. If you encounter such problems, you might need to use a more permissive mode or disable reverse-path filtering altogether.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` command on the VMware virtual appliance host machines to verify that they use IPv4 reverse path filtering.

If the virtual machines use IPv4 reverse path filtering, this command returns the following:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

If your virtual machines are configured correctly, no further action is required.

2 If you need to configure IPv4 reverse path filtering on host machines, open the `/etc/sysctl.conf` file in a text editor.
3 Check the values of the lines that begin with `net.ipv4.conf`

If the values for the following entries are not set to 1 or if they do not exist, add them to the file or update the existing entries accordingly.

```
net.ipv4.conf.all_rp_filter=1
net.ipv4.conf.default_rp_filter=1
```

4 Save the changes and close the file.

**Deny IPv4 Forwarding**

Verify that your VMware appliance host machines deny IPv4 forwarding.

If the system is configured for IP forwarding and is not a designated router, attackers could use it to bypass network security by providing a path for communication not filtered by network devices. Configure your virtual appliance host machines to deny IPv4 forwarding to avoid this risk.

**Procedure**

1 Run the `# cat /proc/sys/net/ipv4/ip_forward` command on the VMware appliance host machines to confirm that they deny IPv4 forwarding.

   If the host machines are configured to deny IPv4 forwarding, this command will return a value of 0 for `/proc/sys/net/ipv4/ip_forward`. If the virtual machines are configured correctly, no further action is necessary.

2 To configure a virtual appliance host machine to deny IPv4 forwarding, open the `/etc/sysctl.conf` file in a text editor.

3 Locate the entry that reads `net.ipv4.ip_forward=0`. If the value for this entry is not currently set to zero or if the entry does not exist, add it or update the existing entry accordingly.

4 Save any changes and close the file.

**Deny IPv6 Forwarding**

As a security best practice, verify that your VMware appliance host systems deny IPv6 forwarding.

If the system is configured for IP forwarding and is not a designated router, attackers could use it to bypass network security by providing a path for communication not filtered by network devices. Configure your virtual appliance host machines to deny IPv6 forwarding to avoid this risk.

**Procedure**

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|grep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 forwarding.

   If the host machines are configured to deny IPv6 forwarding, this command will return the following:

   ```
   /proc/sys/net/ipv6/conf/all/forwarding:0
   /proc/sys/net/ipv6/conf/default/forwarding:0
   ```

   If the host machines are configured correctly, no further action is necessary.
2 If you need to configure a host machine to deny IPv6 forwarding, open the `/etc/sysctl.conf` file in a text editor.

3 Check the values of the lines that begin with `net.ipv6.conf`.

   If the values for the following entries are not set to zero or if the entries do not exist, add the entries or update the existing entries accordingly.

   ```
   net.ipv6.conf.all.accept_redirects=0
   net.ipv6.conf.default.accept_redirects=0
   ```

4 Save any changes you made and close the file.

**Use IPv4 TCP Syncookies**

Verify that your VMware appliance host machines use IPv4 TCP Syncookies.

A TCP SYN flood attack might cause a denial of service by filling a system's TCP connection table with connections in the SYN_RCVD state. Syncookies prevent tracking a connection until receipt of a subsequent ACK, verifying that the initiator is attempting a valid connection and is not a flood source. This technique does not operate in a fully standards-compliant manner, but is only activated during a flood condition, and allows defence of the system while continuing to service valid requests.

**Procedure**

1 Run the `cat /proc/sys/net/ipv4/tcp_syncookies` command on the VMware appliance host machines to verify that they use IPv4 TCP Syncookies.

   If the host machines are configured to deny IPv4 forwarding, this command will return a value of 1 for `/proc/sys/net/ipv4/tcp_syncookies`. If the virtual machines are configured correctly, no further action is necessary.

2 If you need to configure a virtual appliance to use IPv4 TCP Syncookies, open the `/etc/sysctl.conf` in a text editor.

3 Locate the entry that reads `net.ipv4.tcp_syncookies=1`.

   If the value for this entry is not currently set to one or if it does not exist, add the entry or update the existing entry accordingly.

4 Save any changes you made and close the file.

**Deny IPv6 Router Advertisements**

Verify that VMware host machines deny the acceptance of router advertisements and ICMP redirects unless otherwise required for system operation.

IPv6 enables systems to configure their networking devices by automatically using information from the network. From a security perspective, manually configuring important configuration information is preferable to accepting it from the network in an unauthenticated way.
Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` command on the VMware appliance host machines to verify that they deny router advertisements.

   If the host machines are configured to deny IPv6 router advertisements, this command will return values of 0:

   ```
   /proc/sys/net/ipv6/conf/all/accept_ra:0
   /proc/sys/net/ipv6/conf/default/accept_ra:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2 If you need to configure a host machine to deny IPv6 router advertisements, open the `/etc/sysctl.conf` file in a text editor.

3 Check for the following entries.

   ```
   net.ipv6.conf.all.accept_ra=0
   net.ipv6.conf.default.accept_ra=0
   ```

   If these entries do not exist, or if their values are not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes you made and close the file.

Deny IPv6 Router Solicitations

As a security best practice, verify that your VMware appliance host machines deny IPv6 router solicitations unless otherwise required for system operation.

The router solicitations setting determines how many router solicitations are sent when bringing up the interface. If addresses are statically assigned, there is no need to send any solicitations.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitons|egrep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 router solicitations.

   If the host machines are configured to deny IPv6 router advertisements, this command will return the following:

   ```
   /proc/sys/net/ipv6/conf/all/router_solicitons:0
   /proc/sys/net/ipv6/conf/default/router_solicitons:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2 If you need to configure host machines to deny IPv6 router solicitations, open the `/etc/sysctl.conf` file in a text editor.
3 Check for the following entries.

```bash
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes and close the file.

**Deny IPv6 Router Preference in Router Solicitations**

Verify that your VMware appliance host machines to deny IPv6 router solicitations unless otherwise needed for system operation.

The router preference in the solicitations setting determines router preferences. If addresses are statically assigned, there is no need to receive any router preference for solicitations.

**Procedure**

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 router solicitations.

If the host machines are configured to deny IPv6 router advertisements, this command will return the following:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

If the host machines are configured correctly, no further action is necessary.

2 If you need to configure host machines to deny IPv6 route solicitations, open the `/etc/sysctl.conf` file in a text editor.

3 Check for the following entries.

```bash
net.ipv6.conf.all.acceptRaRtrPref=0
net.ipv6.conf.default.acceptRaRtrPref=0
```

If the entries do not exist or if their values not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes you made and close the file.

**Deny IPv6 Router Prefix**

Verify that your VMware appliance host machines deny IPv6 router prefix information unless otherwise required for system operation.

The `accept_ra_pinfo` setting controls whether the system accepts prefix info from the router. If addresses are statically assigned, there is no need to receive any router prefix information.
Procedure

1. Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 router prefix information.

   If the host machines are configured to deny IPv6 router advertisements, this command will return the following.

   ```
   /proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
   /proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2. If you need to configure host machines to deny IPv6 router prefix information, open the `/etc/sysctl.conf` file in a text editor.

3. Check for the following entries.

   ```
   net.ipv6.conf.all.accept_ra_pinfo=0
   net.ipv6.conf.default.accept_ra_pinfo=0
   ```

   If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4. Save any changes and close the file.

Deny IPv6 Router Advertisement Hop Limit Settings

Verify that your VMware appliance host machines deny IPv6 router hop limit settings unless necessary.

The `accept_ra_defrtr` setting controls whether the system will accept Hop Limit settings from a router advertisement. Setting it to zero prevents a router from changing your default IPv6 Hop Limit for outgoing packets.

Procedure

1. Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 router hop limit settings.

   If the host machines are configured to deny IPv6 router hop limit settings, this command will return values of 0.

   ```
   /proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
   /proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2. If you need to configure a host machine to deny IPv6 router hop limit settings, open the `/etc/sysctl.conf` file in a text editor.
3 Check for the following entries.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes you made and close the file.

### Deny IPv6 Router Advertisement Autoconf Settings

Verify that your VMware appliance host machines deny IPv6 router autoconf settings unless necessary.

The `autoconf` setting controls whether router advertisements can cause the system to assign a global unicast address to an interface.

**Procedure**

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` command on the VMware appliance host machines to verify that they deny IPv6 router autoconf settings.

   If the host machines are configured to deny IPv6 router autoconf settings, this command will return values of 0.

   ```
   /proc/sys/net/ipv6/conf/all/autoconf:0
   /proc/sys/net/ipv6/conf/default/autoconf:0
   ```

   If the host machines are configured correctly, no further action is necessary.

2 If you need to configure a host machine to deny IPv6 router autoconf settings, open the `/etc/sysctl.conf` file in a text editor.

3 Check for the following entries.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes you made and close the file.

### Deny IPv6 Neighbor Solicitations

Verify that your VMware appliance host machines to deny IPv6 neighbor solicitations unless necessary.

The `dad_transmits` setting determines how many neighbor solicitations to send out per address (global and link-local) when bringing up an interface to ensure the desired address is unique on the network.
Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` command on the VMware appliance host machines to confirm that they deny IPv6 neighbor solicitations.

   If the host machines are configured to deny IPv6 neighbor solicitations, this command will return values of 0.

   /proc/sys/net/ipv6/conf/all/dad_transmits:0
   /proc/sys/net/ipv6/conf/default/dad_transmits:0

   If the host machines are configured correctly, no further action is necessary.

2 If you need to configure a host machine to deny IPv6 neighbor solicitations, open the `/etc/sysctl.conf` file in a text editor.

3 Check for the following entries.

   net.ipv6.conf.all.dad_transmits=0
   net.ipv6.conf.default.dad_transmits=0

   If the entries do not exist or if their values are not set to zero, add the entries or update the existing entries accordingly.

4 Save any changes you made and close the file.

Restrict IPv6 Max Addresses

Verify that your VMware appliance host machines to restrict IPv6 max address settings to the minimum required for system operation.

The max addresses setting determines how many global unicast IPv6 addresses are available to each interface. The default is 16, but you should set to exactly the number of statically configured global addresses required for your system.

Procedure

1 Run the `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` command on the VMware appliance host machines to verify that they restrict IPv6 max addresses appropriately.

   If the host machines are configured to restrict IPv6 max addresses, this command will return values of 1.

   /proc/sys/net/ipv6/conf/all/max_addresses:1
   /proc/sys/net/ipv6/conf/default/max_addresses:1

   If the host machines are configured correctly, no further action is necessary.

2 If you need to configure IPv6 max addresses on host machines, open the `/etc/sysctl.conf` file in a text editor.
3  Check for the following entries.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

If the entries do not exist or if their values are not set to 1, add the entries or update the existing entries accordingly.

4  Save any changes you made and close the file.

**Configuring Network Settings for the Infrastructure as a Service Host**

As a security best practice, configure network communication settings on your VMware Infrastructure as a Service (IaaS) component host machine according to VMware requirements and guidelines.

Configure the Infrastructure as a Service (IaaS) host machine’s network configuration to support full vRealize Automation functions with appropriate security.

See [Securing the Infrastructure as a Service Component](#).

**Configuring Ports and Protocols**

As a security best practice, configure ports and protocols for all vRealize Automation appliances and components in accordance with VMware guidelines.

Configure incoming and outgoing ports for vRealize Automation components as required for critical system components to operate in production. Disable all unneeded ports and protocols. See [vRealize Automation Reference Architecture](#).

**User Required Ports**

As a security best practice, configure vRealize Automation user ports according to VMware guidelines.

Expose required ports only over a secure network.

<table>
<thead>
<tr>
<th>SERVER</th>
<th>PORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation Appliance</td>
<td>443, 8443</td>
</tr>
</tbody>
</table>

**Administrator Required Ports**

As a security best practice, configure vRealize Automation administrator ports according to VMware guidelines.

Expose required ports only over a secure network.

<table>
<thead>
<tr>
<th>SERVER</th>
<th>PORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Application Services Server</td>
<td>5480</td>
</tr>
</tbody>
</table>

**vRealize Automation Appliance Ports**

As a security best practice, configure incoming and outgoing ports for the vRealize Automation appliance according to VMware recommendations.
Incoming Ports

Configure the minimum required incoming ports for the vRealize Automation appliance. Configure optional ports if needed for your system configuration.

Table 1-4. Minimum Required Incoming Ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Access to the vRealize Automation console and API calls.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Console Proxy (VMRC).</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Access to the virtual appliance Web Management Console.</td>
</tr>
<tr>
<td>5488, 5489</td>
<td>TCP</td>
<td>Internal. Used by the vRealize Automation appliance for updates.</td>
</tr>
<tr>
<td>5672</td>
<td>TCP</td>
<td>RabbitMQ messaging.</td>
</tr>
</tbody>
</table>

Note: When you cluster vRealize Automation appliance instances, you might need to configure the open ports 4369 and 25672.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>40002</td>
<td>TCP</td>
<td>Required for vIDM service. This is firewalled to all external traffic with the exception of traffic from other vRealize Automation appliance nodes when added in HA configuration.</td>
</tr>
</tbody>
</table>

If necessary, configure optional incoming ports.

Table 1-5. Optional Incoming Ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>(Optional) SSH. In a production environment, disable the SSH service listening on port 22, and close port 22.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>(Optional) Redirects to 443.</td>
</tr>
</tbody>
</table>

Outgoing Ports

Configure the required outgoing ports.

Table 1-6. Minimum Required Outgoing Ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>25, 587</td>
<td>TCP, UDP</td>
<td>SMTP for sending outbound notification emails.</td>
</tr>
<tr>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS.</td>
</tr>
<tr>
<td>67, 68, 546, 547</td>
<td>TCP, UDP</td>
<td>DHCP.</td>
</tr>
<tr>
<td>110, 995</td>
<td>TCP, UDP</td>
<td>POP for receiving inbound notification emails.</td>
</tr>
<tr>
<td>143, 993</td>
<td>TCP, UDP</td>
<td>IMAP for receiving inbound notification emails.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Infrastructure as a Service Manager Service over HTTPS.</td>
</tr>
</tbody>
</table>

If necessary, configure optional outgoing ports.
### Table 1-7. Optional Outgoing Ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>(Optional) For fetching software updates. You can download and apply updates separately.</td>
</tr>
<tr>
<td>123</td>
<td>TCP, UDP</td>
<td>(Optional) For connecting directly to NTP instead of using host time.</td>
</tr>
</tbody>
</table>

### Infrastructure as a Service Ports

As a security best practice, configure incoming and outgoing ports for the Infrastructure as a Service (IaaS) components according to VMware guidelines.

#### Incoming Ports

Configure the minimum required incoming ports for the IaaS components.

**Table 1-8. Minimum Required Incoming Ports**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Service</td>
<td>443</td>
<td>TCP</td>
<td>Communication with IaaS components and vRealize Automation Appliance over HTTPS. Any virtualization hosts that proxy agents manage must also have TCP port 443 open for incoming traffic</td>
</tr>
</tbody>
</table>

#### Outgoing Ports

Configure the minimum required outgoing ports for the IaaS components.

**Table 1-9. Minimum Required Outgoing Ports**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS.</td>
</tr>
<tr>
<td>All</td>
<td></td>
<td>TCP, UDP</td>
<td>DHCP.</td>
</tr>
<tr>
<td>Manager Service</td>
<td>443</td>
<td>TCP</td>
<td>Communication with vRealize Automation Appliance over HTTPS.</td>
</tr>
<tr>
<td>Web site</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS.</td>
</tr>
<tr>
<td>Distributed Execution Managers</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS.</td>
</tr>
<tr>
<td>Proxy Agents</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service and virtualization hosts over HTTPS.</td>
</tr>
<tr>
<td>Guest Agent</td>
<td>443</td>
<td>TCP</td>
<td>Communication with Manager Service over HTTPS.</td>
</tr>
<tr>
<td>Manager Service, Web site</td>
<td>1433</td>
<td>TCP</td>
<td>MSSQL.</td>
</tr>
</tbody>
</table>

If needed, configure optional outgoing ports.

**Table 1-10. Optional Outgoing Ports**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>PORT</th>
<th>PROTOCOL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>123</td>
<td>TCP, UDP</td>
<td>NTP is optional.</td>
</tr>
</tbody>
</table>
Auditing and Logging

As a security best practice, set up auditing and logging on your vRealize Automation system in accordance with VMware recommendations.

Remote logging to a central log host provides a secure store for log files. By gathering log files to a central host, you can monitor the environment with a single tool. Also, you can perform aggregate analysis and search for evidence of threats such as coordinated attacks on multiple entities within the infrastructure. Logging to a secure, centralized log server can help prevent log tampering, and also provides a long-term audit record.

Ensure That the Remote Logging Server Is Secure

Often, after attackers breach the security of your host machine, they attempt to search for and tamper with log files to cover their tracks and maintain control without being discovered. Securing the remote logging server appropriately helps to discourage log tampering.

Use an Authorized NTP Server

Ensure that all host machines use the same relative time source, including the relevant localization offset, and that you can correlate the relative time source to an agreed-upon time standard such as Coordinated Universal Time (UTC). A disciplined approach to time sources enables you to quickly track and correlate an intruder's actions when you review the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks and can make auditing inaccurate.

Use at least three NTP servers from outside time sources or configure a few local NTP servers on a trusted network that in turn obtain their time from at least three outside time sources.

Installing vRealize Automation

Follow the instructions provided to install a new instance of vRealize Automation.

vRealize Automation Installation Overview

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

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

About vRealize Automation Installation

You can install vRealize Automation through different means, each with varying levels of interactivity.
To install, you deploy a vRealize Automation appliance and then complete the actual installation using one of the following options:

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

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

New in this vRealize Automation Installation

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

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

vRealize Automation Installation Components

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

The vRealize Automation Appliance

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

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

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

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

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

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

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

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

**Infrastructure as a Service**

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

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

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

**Web Server**

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

**Model Manager**

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

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

**Manager Service**

The Manager Service is a Windows service that coordinates communication between IaaS DEMs, the SQL Server database, agents, and SMTP. In addition, the Manager Service communicates with the Web server through the Model Manager and must be run under a domain account with local administrator privileges on all IaaS Windows servers.
Unless you enable automatic Manager Service failover, IaaS requires that only one Windows machine actively runs the Manager Service at a time. For backup or high availability, you may deploy additional Manager Service machines, but the manual failover approach requires that backup machines have the service stopped and configured to start manually.

For more information, see About Automatic Manager Service Failover.

**SQL Server Database**

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

**Distributed Execution Manager**

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

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

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

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

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

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

**Agents**

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

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

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

A virtualization proxy agent has the following characteristics.

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

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

Virtual Desktop Integration Agents

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

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

External Provisioning Integration Agents

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

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

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

Windows Management Instrumentation Agent

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

Deployment Type

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

Minimal vRealize Automation Deployments

Minimal deployments include one vRealize Automation appliance and one Windows server that hosts the IaaS components. In a minimal deployment, the vRealize Automation SQL Server database can be on the same IaaS Windows server with the IaaS components, or on a separate Windows server.
You cannot convert a minimal deployment to an enterprise deployment. To scale a deployment up, start with a small enterprise deployment, and add components to that. Starting with a minimal deployment is not supported.

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

**Distributed vRealize Automation Deployments**

Distributed, enterprise deployments can be of varying size. A basic distributed deployment might improve vRealize Automation simply by hosting IaaS components on separate Windows servers as shown in the following figure.
Many production deployments go even further, with redundant appliances, redundant servers, and load balancing for even more capacity. Large, distributed deployments provide for better scale, high availability, and disaster recovery. Note that the embedded instance of vRealize Orchestrator is now recommended, but you might see vRealize Automation connected to an external vRealize Orchestrator in older deployments.
Figure 1-12. Large Distributed and Load Balanced vRealize Automation Deployment

For more information about scalability and high availability, see the vRealize Automation Reference Architecture guide.
Choosing Your Installation Method

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

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

Preparing for vRealize Automation Installation

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

General Preparation

There are several deployment-wide considerations to be aware of before installing vRealize Automation. For more about high-level environment requirements, including supported operating system and browser versions, see the vRealize Automation Support Matrix.

User Web Browsers

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

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

Third Party Software

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

Time Synchronization

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

- The vRealize Automation appliance host
- One external network time protocol (NTP) server
To use the vRealize Automation appliance host, you must run NTP on the ESXi host. For more about timekeeping, see VMware Knowledge Base article 1318.

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

**Accounts and Passwords**

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

**IaaS Service Account**

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

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

  - If you use the installer to create the database, in SQL, add the sysadmin role to the account before installation.
    
    The sysadmin role is not required if you choose to use a pre-existing empty database.

**IIS Application Pool Identity**

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

**IaaS Database Credentials**

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

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

**IaaS Database Security Passphrase**

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

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

**vSphere Endpoints**

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

**vRealize Automation Administrator Password**

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

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

**Host Names and IP Addresses**

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

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

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

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

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

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

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

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

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

**Latency and Bandwidth**

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

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

- vRealize Automation appliance
- IaaS Web server
- IaaS Model Manager host
- IaaS Manager Service host
- IaaS SQL Server database
- IaaS DEM Orchestrator

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

- IaaS DEM Worker

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

- IaaS Proxy Agent

**vRealize Automation Appliance**

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

The minimum virtual machine hardware on which you can deploy is Version 7, or ESX/ESXi 4.x or later. See VMware Knowledge Base article 2007240. Because of the hardware resource demand, do not deploy on VMware Workstation.
After deployment, you might use vSphere to adjust vRealize Automation appliance hardware settings to meet Active Directory requirements. See the following table.

Table 1-11. vRealize Automation Appliance Hardware Requirements for Active Directory

<table>
<thead>
<tr>
<th>vRealize Automation Appliance for Small Active Directories</th>
<th>vRealize Automation Appliance for Large Active Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 CPUs</td>
<td>4 CPUs</td>
</tr>
<tr>
<td>18 GB memory</td>
<td>22 GB memory</td>
</tr>
<tr>
<td>60 GB disk storage</td>
<td>60 GB disk storage</td>
</tr>
</tbody>
</table>

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

vRealize Automation Appliance Ports

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

The following ports are used by the vRealize Automation appliance.

Table 1-12. Incoming Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Optional. Access for SSH sessions.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Optional. Redirects to 443.</td>
</tr>
<tr>
<td>88</td>
<td>TCP (UDP optional)</td>
<td>Cloud KDC Kerberos authentication from external mobile devices.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Access to the vRealize Automation console and API calls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access for machines to download the guest agent and software bootstrap agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access for load balancer, browser.</td>
</tr>
<tr>
<td>4369, 5671, 5672, 25672</td>
<td>TCP</td>
<td>RabbitMQ messaging.</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Access to the virtual appliance management interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used by the Management Agent.</td>
</tr>
<tr>
<td>5488, 5489</td>
<td>TCP</td>
<td>Internally used by the vRealize Automation appliance for updates.</td>
</tr>
<tr>
<td>8230, 8280, 8281, 8283</td>
<td>TCP</td>
<td>Internal vRealize Orchestrator instance.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Access for browser. Identity Manager administrator port over HTTPS.</td>
</tr>
<tr>
<td>8444</td>
<td>TCP</td>
<td>Console proxy communication for vSphere VMware Remote Console connections.</td>
</tr>
<tr>
<td>9300–9400</td>
<td>TCP</td>
<td>Access for Identity Manager audits.</td>
</tr>
<tr>
<td>54328</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-13. Outgoing Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>25, 587</td>
<td>TCP, UDP</td>
<td>SMTP for sending outbound notification email.</td>
</tr>
<tr>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS server.</td>
</tr>
<tr>
<td>67, 68, 546, 547</td>
<td>TCP, UDP</td>
<td>DHCP.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Optional. For fetching software updates. Updates can be downloaded separately and applied.</td>
</tr>
<tr>
<td>88, 464, 135</td>
<td>TCP, UDP</td>
<td>Domain controller.</td>
</tr>
<tr>
<td>110, 995</td>
<td>TCP, UDP</td>
<td>POP for receiving inbound notification email.</td>
</tr>
<tr>
<td>143, 993</td>
<td>TCP, UDP</td>
<td>IMAP for receiving inbound notification email.</td>
</tr>
<tr>
<td>123</td>
<td>TCP, UDP</td>
<td>Optional. For connecting directly to NTP instead of using host time.</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>Access to View Connection Server.</td>
</tr>
<tr>
<td>389, 636, 3268, 3269</td>
<td>TCP</td>
<td>Active Directory. Default ports shown, but are configurable.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Communication with IaaS Manager Service and infrastructure endpoint hosts over HTTPS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication with the vRealize Automation software service over HTTPS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access to the Identity Manager upgrade server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access to View Connection Server.</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>Access to ThinApp repository for Identity Manager.</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>ESXi network file copy operations and VMware Remote Console connections.</td>
</tr>
<tr>
<td>5050</td>
<td>TCP</td>
<td>Optional. For communicating with vRealize Business for Cloud.</td>
</tr>
<tr>
<td>5432</td>
<td>TCP, UDP</td>
<td>Optional. For communicating with another appliance PostgreSQL database.</td>
</tr>
<tr>
<td>5500</td>
<td>TCP</td>
<td>RSA SecurID system. Default port shown, but is configurable.</td>
</tr>
<tr>
<td>8281</td>
<td>TCP</td>
<td>Optional. For communicating with an external vRealize Orchestrator instance.</td>
</tr>
<tr>
<td>9300–9400</td>
<td>TCP</td>
<td>Access for Identity Manager audits.</td>
</tr>
<tr>
<td>54328</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>

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

### IaaS Windows Servers

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

- Place all IaaS Windows servers on the same domain. Do not use Workgroups.
- Each server needs the following minimum hardware.
  - 2 CPUs
  - 8 GB memory
- 40 GB disk storage
  A server that hosts the SQL database together with IaaS components might need additional hardware.
- Because of the hardware resource demand, do not deploy on VMware Workstation.
- Install Microsoft .NET Framework 3.5.
- Install Microsoft .NET Framework 4.5.2 or later.

A copy of .NET is available from any vRealize Automation appliance:
If you use Internet Explorer for the download, verify that Enhanced Security Configuration is disabled.
- Install Microsoft PowerShell 2.0, 3.0, or 4.0, based on your version of Windows.
  Note that some vRealize Automation upgrades or migrations might require an older or newer PowerShell version, in addition to the one that you are currently running.
- If you install more than one IaaS component on the same Windows server, plan to install them to the same installation folder. Do not use different paths.
- IaaS servers use TLS for authentication, which is enabled by default on some Windows servers.
  Some sites disable TLS for security reasons, but you must leave at least one TLS protocol enabled.
  This version of vRealize Automation supports TLS 1.2.
- Enable the Distributed Transaction Coordinator (DTC) service. IaaS uses DTC for database transactions and actions such as workflow creation.

  **Note** If you clone a machine to make an IaaS Windows server, install DTC on the clone after cloning. If you clone a machine that already has DTC, its unique identifier is copied to the clone, which causes communication to fail. See Error in Manager Service Communication.

Also enable DTC on the server that hosts the SQL database, if it is separate from IaaS. For more about DTC enablement, see VMware Knowledge Base article 2038943.
- Verify that the Secondary Log On service is running. If desired, you may stop the service after installation is complete.

**IaaS Windows Server Ports**
Ports on the IaaS Windows servers must be configured before vRealize Automation installation.
Open ports between all IaaS Windows servers according to the following tables. Include the server that hosts the SQL database, if it is separate from IaaS. Alternatively, if site policies allow, you may disable firewalls between IaaS Windows servers and SQL Server.
### Table 1-14. Incoming Ports

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

### Table 1-15. Outgoing Ports

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

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

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

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

- Configure Java.
  - Install 64-bit Java 1.8 update 161 or later. Do not use 32-bit.
    The JRE is enough. You do not need the full JDK.
  - Set the JAVA_HOME environment variable to the Java installation folder.
  - Verify that %JAVA_HOME%\bin\java.exe is available.
- Configure Internet Information Services (IIS) according to the following table.

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

**Table 1-16. IaaS Manager Service Host Internet Information Services**

<table>
<thead>
<tr>
<th>IIS Component</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Information Services (IIS) roles</td>
<td>- Windows Authentication</td>
</tr>
<tr>
<td></td>
<td>- Static Content</td>
</tr>
<tr>
<td></td>
<td>- Default Document</td>
</tr>
<tr>
<td></td>
<td>- ASPNET 3.5 and ASPNET 4.5</td>
</tr>
<tr>
<td></td>
<td>- ISAPI Extensions</td>
</tr>
<tr>
<td></td>
<td>- ISAPI Filter</td>
</tr>
<tr>
<td>IIS Windows Process Activation Service roles</td>
<td>- Configuration API</td>
</tr>
<tr>
<td></td>
<td>- Net Environment</td>
</tr>
<tr>
<td></td>
<td>- Process Model</td>
</tr>
<tr>
<td></td>
<td>- WCF Activation (Windows 2008 variants only)</td>
</tr>
<tr>
<td></td>
<td>- HTTP Activation</td>
</tr>
<tr>
<td></td>
<td>- Non-HTTP Activation (Windows 2008 variants only)</td>
</tr>
<tr>
<td></td>
<td>(Windows 2012 variants: Go to Features &gt; .Net Framework 3.5 Features &gt; Non-HTTP Activation)</td>
</tr>
<tr>
<td>IIS Authentication settings</td>
<td>Set the following non-defaults.</td>
</tr>
<tr>
<td></td>
<td>- Windows Authentication enabled</td>
</tr>
<tr>
<td></td>
<td>- Anonymous Authentication disabled</td>
</tr>
<tr>
<td></td>
<td>Do not change the following defaults.</td>
</tr>
<tr>
<td></td>
<td>- Negotiate Provider enabled</td>
</tr>
<tr>
<td></td>
<td>- NTLM Provider enabled</td>
</tr>
<tr>
<td></td>
<td>- Windows Authentication Kernel Mode enabled</td>
</tr>
<tr>
<td></td>
<td>- Windows Authentication Extended Protection disabled</td>
</tr>
<tr>
<td></td>
<td>- For certificates using SHA512, TLS1.2 must be disabled on Windows 2012 variants</td>
</tr>
</tbody>
</table>

**IaaS Manager Service Host**

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

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

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

- The Manager Service host must be able to resolve the NETBIOS name of the SQL Server database host. If it cannot resolve the NETBIOS name, add the SQL Server NETBIOS name to the Manager Service machine /etc/hosts file.
IaaS SQL Server Host

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

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

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

- AlwaysOn Availability Group (AAG) is only supported with SQL Server 2016 Enterprise. When you use AAG, you specify the AAG listener FQDN as the SQL Server host.

- When hosted together with IaaS components, configure Java.
  
  - Install 64-bit Java 1.8 update 161 or later. Do not use 32-bit.
    
    The JRE is enough. You do not need the full JDK.
  
  - Set the JAVA_HOME environment variable to the Java installation folder.
  
  - Verify that %JAVA_HOME%/bin/java.exe is available.

- Use a supported SQL Server version from the vRealize Automation Support Matrix.

- Enable TCP/IP protocol for SQL Server.

- SQL Server includes a model database that is the template for all databases created on the SQL instance. For IaaS to install correctly, do not change the model database size.

- Usually, the server needs more hardware than the minimums described in IaaS Windows Servers.
  
  For more information, see vRealize Automation Hardware Specifications and Capacity Maximums.

- Before running the vRealize Automation installer, you need to identify accounts and add permissions in SQL. See Accounts and Passwords.

IaaS Distributed Execution Manager Host

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

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

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

DEM Workers with Amazon Web Services

A vRealize Automation IaaS DEM Worker that communicates with Amazon Web Services (AWS) must meet additional requirements, in addition to those for all IaaS Windows servers and DEMs in general.
A DEM Worker can communicate with AWS for provisioning. The DEM Worker communicates with, and collects data from, an Amazon EC2 account.

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

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

**DEM Workers with Openstack or PowerVC**

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

**Table 1-17. DEM Worker Openstack and PowerVC Requirements**

<table>
<thead>
<tr>
<th>Your Installation</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>In Windows Registry, enable TLS v1.2 support for .NET framework. For example:</td>
</tr>
<tr>
<td></td>
<td><code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319</code> &quot;SchUseStrongCrypto&quot;=dword:00000001</td>
</tr>
<tr>
<td></td>
<td><code>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319</code> &quot;SchUseStrongCrypto&quot;=dword:00000001</td>
</tr>
<tr>
<td>Windows 2008 DEM Host</td>
<td>In Windows Registry, enable TLS v1.2 protocol. For example:</td>
</tr>
<tr>
<td></td>
<td><code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client</code> &quot;DisabledByDefault&quot;=dword:00000000 &quot;Enabled&quot;=dword:00000001</td>
</tr>
<tr>
<td></td>
<td><code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server</code> &quot;DisabledByDefault&quot;=dword:00000000 &quot;Enabled&quot;=dword:00000001</td>
</tr>
<tr>
<td>Self-signed certificates on your infrastructure endpoint host</td>
<td>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.</td>
</tr>
</tbody>
</table>
DEM Workers with Red Hat Enterprise Virtualization

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

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

DEM Workers with SCVMM

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

- Install the DEM Worker on the same machine with the SCVMM console.
  
  A best practice is to install the SCVMM console on a separate DEM Worker.
- The DEM worker must have access to the SCVMM PowerShell module installed with the console.
- The PowerShell Execution Policy must be set to RemoteSigned or Unrestricted.
  
  To verify the PowerShell Execution Policy, enter one of the following commands at the PowerShell command prompt.

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

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

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

The following additional requirements apply to SCVMM.

- vRealize Automation supports SCVMM 2012 R2, which requires PowerShell 3 or later.
- Install the SCVMM console before you install vRealize Automation DEM Workers that consume SCVMM work items.
  
  If you install the DEM Worker before the SCVMM console, you see log errors similar to the following example.
Workflow 'ScvmmEndpointDataCollection' failed with the following exception: The term 'Get-VMMServer' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

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

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

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

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

For additional information about preparing for machine provisioning, see Preparing Your SCVMM Environment.

Certificates

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

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

**Note** vRealize Automation supports SHA2 certificates. The self-signed certificates generated by the system use SHA-256 With RSA Encryption. You might need to update to SHA2 certificates due to operating system or browser requirements.
You can update or replace certificates after deployment. For example, a certificate may expire or you may choose to use self-signed certificates during your initial deployment, but then obtain certificates from a trusted authority before going live with your vRealize Automation implementation.

**Table 1-18. Certificate Implementations**

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

**Certificate Chains**

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

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

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

**Certificate Changes if Customizing the vRealize Automation Login URL**

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

**vRealize Automation Certificate Requirements**

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

**Supported Certificate Types**

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

The following requirements address common identity format and certificate types used with typical vRealize Automation deployments.
<table>
<thead>
<tr>
<th>Certificate Property</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Algorithm</td>
<td>SHA1, SHA2, (256, 584, 512)</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>RSASSA-PKCS1_V1_5</td>
</tr>
<tr>
<td>Key Length</td>
<td>2084, 4096</td>
</tr>
</tbody>
</table>

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

### vRealize Automation Certificate Support Matrix

<table>
<thead>
<tr>
<th>Hash Algorithm</th>
<th>SHA1</th>
<th>SHA2-256</th>
<th>SHA2-384</th>
<th>SHA2-512</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>RSASSA-PKCS1_V1_5</td>
<td>RSASSA-PSS</td>
<td>RSASSA-PKCS1_V1_5</td>
<td>RSASSA-PSS</td>
</tr>
<tr>
<td>Key Size</td>
<td>2048</td>
<td>4096</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td>vRealize Automation Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hash Algorithm</th>
<th>SHA2-384</th>
<th>SHA2-512</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>RSASSA-PKCS1_V1_5</td>
<td>RSASSA-PSS</td>
</tr>
<tr>
<td>Key Size</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td>vRealize Automation Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

### 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 1-19. Sample Certificate Values and Commands (openssl)**

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

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

About vRealize Automation Appliance Deployment

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

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

Deploy the vRealize Automation Appliance

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

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

Prerequisites

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

Procedure

1. Select the vSphere Deploy OVF Template option.
2. Enter the path to the vRealize Automation appliance .ovf or .ova file.
3. Review the template details.
4. Read and accept the end-user license agreement.
5. Enter an appliance name and inventory location.
   - When you deploy appliances, use a different name for each one, and do not include non-alphanumeric characters such as underscores (_) in names.
6. Select the host and cluster in which the appliance will reside.
7 Select the resource pool in which the appliance will reside.
8 Select the storage that will host the appliance.
9 Select a disk format.
   Thick formats improve performance, and thin formats save storage space.
   Format does not affect appliance disk size. If an appliance needs more space for data, add disk by using vSphere after deploying.
10 From the drop-down menu, select a Destination Network.
11 Complete the appliance properties.
   a Enter and confirm a root password.
      The root account credentials log you in to the browser-based administration interface hosted by the appliance, or the appliance operating system command-line console.
   b Select whether or not to allow remote SSH connections to the command-line console.
      Disabling SSH is more secure but requires that you access the console directly in vSphere instead of through a separate terminal client.
c  For **Hostname**, enter the appliance FQDN. For best results, enter the FQDN even if using DHCP.

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

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

**Figure 1-13. Example Virtual Appliance Properties**

<table>
<thead>
<tr>
<th><strong>Application</strong></th>
<th>3 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSH service in the appliance</td>
<td>This will be used as an initial status of the SSH service in the appliance. You can change the appliance Web console.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>The host name for this virtual machine. Provide the fully qualified domain name if you use DNS. Leave blank to try to reverse look up the IP address if you use DHCP.</td>
</tr>
<tr>
<td>Initial root password</td>
<td>This will be used as an initial password for the root user account. You can change the password using the passwd command or from the appliance Web console.</td>
</tr>
<tr>
<td>Enter password</td>
<td>************</td>
</tr>
<tr>
<td>Confirm password</td>
<td>************</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Networking Properties</strong></th>
<th>6 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>The default gateway address for this VM. Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>12.34.56.79</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name of this VM. Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>mycompany.com</td>
</tr>
<tr>
<td>Domain Name Servers</td>
<td>The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>12.34.56.80, 12.34.56.81</td>
</tr>
<tr>
<td>Domain Search Path</td>
<td>The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>mycompany.com</td>
</tr>
<tr>
<td>Network 1 IP Address</td>
<td>The IP address for this interface. Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>12.34.56.78</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>The netmask or prefix for this interface. Leave blank if DHCP is desired.</td>
</tr>
<tr>
<td></td>
<td>255.255.254.0</td>
</tr>
</tbody>
</table>
12 Depending on your deployment, vCenter Server, and DNS configuration, select one of the following ways of finishing deployment and powering up the appliance.

- If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.
  a. Select **Power on after deployment** and click **Finish**.
  b. After the file finishes deploying into vCenter Server, click **Close**.
  c. Wait for the virtual machine to start, which might take up to 5 minutes.

- If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
  a. After the file finishes deploying into vCenter Server, click **Close**.
  b. Power on the vRealize Automation appliance.
  c. Wait for the virtual machine to start, which might take up to 5 minutes.
  d. Verify that the vRealize Automation appliance is deployed by pinging its FQDN. If you cannot ping the appliance, restart the virtual machine.
  e. Wait for the virtual machine to start, which might take up to 5 minutes.

- If you deployed the vRealize Automation appliance to vCloud using vCloud Director, vCloud might override the password that you entered during OVA deployment. To prevent the override, take the following steps.
  a. After deploying in vCloud Director, click your vApp to view the vRealize Automation appliance.
  b. Right-click the vRealize Automation appliance, and select **Properties**.
  c. Click the **Guest OS Customization** tab.
  d. Under **Password Reset**, clear the **Allow local administrator password** option, and click **OK**.
  e. Power on the vRealize Automation appliance.
  f. Wait for the virtual machine to start, which might take up to 5 minutes.

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

**What to do next**

- (Optional) Add NICs. See Add Network Interface Controllers Before Running the Installer.
- Log in to the browser-based administration interface to run the consolidated Installation Wizard or to manually configure the appliance.
  
  https://vrealize-automation-appliance-FQDN:5480

- Alternatively, you can skip logging in so that you can take advantage of vRealize Automation silent or API based installation.
Add Network Interface Controllers Before Running the Installer

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

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

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

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

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

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

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

Prerequisites

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

Procedure

1. In vCenter, add NICs to each vRealize Automation appliance.
   a. Right click the newly deployed appliance and select Edit Settings.
   b. Add VMXNET3 NICs.
   c. If it is powered on, restart the appliance.
2. Log in to the vRealize Automation appliance command line as root.
3. Configure the NICs by running the following command for each NIC.

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

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

   For example:

   /opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20 255.255.255.0 192.168.100.1
4 Verify that all vRealize Automation nodes can resolve each other by DNS name.

5 Verify that all vRealize Automation nodes can access any load balanced FQDNs for vRealize Automation components.

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

7 In vCenter, add NICs to IaaS Windows servers.
   a Right click the IaaS server and select Edit Settings.
   b Add NICs to the IaaS server virtual machine.

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

What to do next

- (Optional) If you need static routes, follow the guidelines in Configure Static Routes before continuing with installation.
- Log in to the browser-based administration interface to run the consolidated Installation Wizard or to manually configure the appliance.
  
  https://vrealize-automation-appliance-FQDN:5480
- Alternatively, you can skip logging in so that you can take advantage of vRealize Automation silent or API based installation.

Installing vRealize Automation with the Installation Wizard

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

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

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

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

Using the Installation Wizard for Minimal Deployments

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

Install a minimal deployment for proof-of-concept work or to become familiar with vRealize Automation.
Start the Installation Wizard for a Minimal Deployment

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

Prerequisites

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

Procedure

1. Log in as root to the vRealize Automation appliance administration interface.
   
   https://vrealize-automation-appliance-FQDN:5480

2. When the Installation Wizard appears, click Next.

3. Accept the license agreement and click Next.

4. On the Deployment Type page, select Minimal deployment and Install Infrastructure as a Service, and click Next.

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

What to do next

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

Install the vRealize Automation Management Agent

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

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

The Management Agent registers the IaaS Windows server with the specific vRealize Automation appliance, automates the installation and management of IaaS components, and collects support and telemetry information. The Management Agent runs as a Windows service under a domain account with administrator rights on IaaS Windows servers.

Prerequisites

Create a vRealize Automation appliance and begin the Installation Wizard.

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

1. Log in to the vRealize Automation appliance console as root.
2. Enter the following command:
   `openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1`
3. Copy the fingerprint so that you can verify it later. For example:
4. Log in to the IaaS Windows server using an account that has administrator rights.
5. Open a Web browser to the vRealize Automation appliance installer URL.
   `https://vrealize-automation-appliance-FQDN:5480/installer`
6. Click **Management Agent installer**, and save and run the `.msi` file.
7. Read the welcome.
8. Accept the end user license agreement.
9. Accept or change the installation folder.
   `Program Files (x86)\VMware\vCAC\Management Agent`
10. Enter vRealize Automation appliance details:
    a. Enter the appliance HTTPS address, including FQDN and :5480 port number.
    b. Enter the appliance root account credentials.
    c. Click **Load**, and confirm that the fingerprint matches the one you copied earlier. Ignore colons.
       If the fingerprints do not match, verify that you have the correct appliance address.

   ![Figure 1-14. Management Agent—vRealize Automation Appliance Details](image)

11. Enter the domain\username and password for the service account.
    The service account must be a domain account with administrator rights on IaaS Windows servers. Use the same service account throughout.
Follow the prompts to finish installing the Management Agent.

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

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

**What to do next**

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

**Completing the Installation Wizard**

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

- When you finish the wizard, the last page displays the path and name to a properties file. You can edit the file and use it to perform a silent vRealize Automation installation with the same or similar settings from your wizard session. See [Silent vRealize Automation Installation](#).
- If you created initial content, you can log in to the default tenant as the configurationadmin user and request the catalog items. For an example of how to request the item and complete the manual user action, see [Scenario: Request Initial Content for a Rainpole Proof of Concept Deployment](#).
- To configure access to the default tenant for other users, see [Configure Access to the Default Tenant](#).

**Using the Installation Wizard for Enterprise Deployments**

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

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

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

**Start the Installation Wizard for an Enterprise Deployment**

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

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

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

Procedure

1. Log in as root to the vRealize Automation appliance administration interface.
   ```shell
   https://vrealize-automation-appliance-FQDN:5480
   ```
2. When the Installation Wizard appears, click Next.
3. Accept the End User License Agreement and click Next.
4. On the Deployment Type page, select Enterprise deployment and Install Infrastructure as a Service.
5. On the Installation Prerequisites page, you pause to log in to your IaaS Windows servers and install the Management Agent. The Management Agent allows the vRealize Automation appliance to discover and connect to those IaaS servers.

What to do next

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

Install the vRealize Automation Management Agent

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

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

The Management Agent registers the IaaS Windows server with the specific vRealize Automation appliance, automates the installation and management of IaaS components, and collects support and telemetry information. The Management Agent runs as a Windows service under a domain account with administrator rights on IaaS Windows servers.

Prerequisites

Create a vRealize Automation appliance and begin the Installation Wizard.

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

Procedure

1. Log in to the vRealize Automation appliance console as root.
2. Enter the following command:
   ```shell
   openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
   ```
3 Copy the fingerprint so that you can verify it later. For example:
4 Log in to the IaaS Windows server using an account that has administrator rights.
5 Open a Web browser to the vRealize Automation appliance installer URL.
   https://vrealize-automation-appliance-FQDN:5480/installer
6 Click **Management Agent installer**, and save and run the .msi file.
7 Read the welcome.
8 Accept the end user license agreement.
9 Accept or change the installation folder.
   Program Files (x86)\VMware\vCAC\Management Agent
10 Enter vRealize Automation appliance details:
   a Enter the appliance HTTPS address, including FQDN and :5480 port number.
   b Enter the appliance root account credentials.
   c Click **Load**, and confirm that the fingerprint matches the one you copied earlier. Ignore colons.
      If the fingerprints do not match, verify that you have the correct appliance address.

   **Figure 1-15. Management Agent—vRealize Automation Appliance Details**

   vRA appliance address:
   [https://va1.company.com:5480](https://va1.company.com:5480)
   Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5480
   Root username:  Password: ********
   Management Site Service certificate SHA1 fingerprint:
   718447720357C8C2686500006BCD823969254BF89
   I confirm the fingerprint matches the Management Site Service SSL certificate

11 Enter the domain\username and password for the service account.
   The service account must be a domain account with administrator rights on IaaS Windows servers.
   Use the same service account throughout.
12 Follow the prompts to finish installing the Management Agent.
Repeat the procedure for all Windows servers that will host IaaS components.

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

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

**What to do next**

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

**Completing the Installation Wizard**

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

- When you finish the wizard, the last page displays the path and name to a properties file. You can edit the file and use it to perform a silent vRealize Automation installation with the same or similar settings from your wizard session. See Silent vRealize Automation Installation.
- If you created initial content, you can log in to the default tenant as the configurationadmin user and request the catalog items. For an example of how to request the item and complete the manual user action, see Scenario: Request Initial Content for a Rainpole Proof of Concept Deployment.
- To configure access to the default tenant for other users, see Configure Access to the Default Tenant.

**Step Through the vRealize Automation Installation Wizard**

The vRealize Automation Installation Wizard presents you with easy to use pages where you check for prerequisites, enter settings, validate settings, and install vRealize Automation components.

**Note** The wizard includes steps where you pause to log in to other systems, such as load balancers or IaaS Windows servers.

**Prerequisites**

- Create one or more unconfigured appliances. See Deploy the vRealize Automation Appliance.

  Minimal deployments use one vRealize Automation appliance. Enterprise deployments may have multiple appliances behind load balancing.

- Have one or more Windows systems available on which to host IaaS components.

- Start the wizard by logging in as root to the vRealize Automation appliance administration interface.  
  
  https://vrealize-automation-appliance-FQDN:5480
Procedure

1 **Deployment Type**
   On the Deployment Type page, you decide which vRealize Automation components, and how many of each, you want to install.

2 **Installation Prerequisites**
   On the Installation Prerequisites page, you pause to establish a connection to Windows machines that will host vRealize Automation IaaS. In addition, you select a time synchronization source.

3 **vRealize Appliances**
   (Enterprise Deployments Only) On the vRealize Appliances page, you have the option to create a high-availability deployment with multiple vRealize Automation appliances.

4 **Server Roles**
   (Enterprise Deployments Only) On the Server Roles page, you assign vRealize Automation IaaS component roles to the Windows machines where you had installed the Management Agent earlier.

5 **Prerequisite Checker**
   On the Prerequisite Checker page, you check and fix your vRealize Automation Windows servers to support IaaS installation.

6 **vRealize Automation Host**
   On the vRealize Automation Host page, you set the base URL address for vRealize Automation. The address is usually the vRealize Automation appliance or, in high availability deployments, a load balancer.

7 **Single Sign On**
   On the Single Sign On page, you set the vRealize Automation default tenant system administrator log in credentials.

8 **IaaS Host**
   On the IaaS Host page, you set the base URL addresses for certain IaaS components. In addition, you create a security passphrase for the vRealize Automation IaaS SQL database.

9 **Microsoft SQL Server**
   On the Microsoft SQL Server page, you configure the vRealize Automation IaaS SQL database. The IaaS database records provisioned machines, associated elements, and policies.

10 **Web Role**
    (Enterprise Deployments Only) On the Web Role page, you separately configure the vRealize Automation IaaS Web site in IIS.

11 **Manager Service Role**
    (Enterprise Deployments Only) On the Manager Service Role page, you configure the separate vRealize Automation Windows machine that hosts the IaaS Manager Service.
12 **Distributed Execution Managers**
   On the Distributed Execution Managers page, you configure the vRealize Automation Windows machines that host IaaS DEMs. Multiple DEM hosts are supported.

13 **Agents**
   On the Agents page, you create the linkage between vRealize Automation IaaS and the virtualization resources onto which infrastructure is deployed. You select an agent type, and complete the details for the corresponding endpoint.

14 **vRealize Appliance Certificate**
   On the vRealize Appliance Certificate page, you create or select the authentication certificate that the vRealize Automation appliance uses. When the certificate is self-signed, end users see and confirm it when they log in to vRealize Automation in a browser.

15 **Web Certificate**
   On the Web Certificate page, you create or select the authentication certificate that the IaaS Web server uses. The vRealize Automation appliance connects to the Web server and needs to authenticate and trust it.

16 **Manager Service Certificate**
   (Enterprise Deployments Only) On the Manager Service Certificate page, you create or select the authentication certificate that the vRealize Automation IaaS Manager Service host uses. The other IaaS Windows servers connect to the Manager Service host and need to authenticate and trust it.

17 **Load Balancers**
   (Enterprise Deployments Only) On the Load Balancers page, you pause to configure load balancers for the correct pool of vRealize Automation member systems.

18 **Validation**
   On the Validation page, you verify that vRealize Automation installation can proceed.

19 **Create Snapshots**
   On the Create Snapshots page, you pause to take virtual machine snapshots of all vRealize Automation components before proceeding with installation.

20 **Installation Details**
   On the Installation Details page, you start the vRealize Automation installation or retry it if problems occurred.

21 **Licensing**
   On the Licensing page, you enter a key to activate the installed vRealize Automation product.

22 **Telemetry**
   On the Telemetry page, you decide whether or not vRealize Automation sends usage statistics to VMware as part of the Customer Experience Improvement Program.
Post Installation Options
On the Post Installation Options page, you have options for creating new vRealize Automation data or migrating older deployment data to your new installation.

Initial Content Configuration
On the Initial Content Configuration page, you create a new, local vRealize Automation default tenant user who can begin a content workflow for a vSphere endpoint.

Migration Configuration
On the Migration Configuration page, you can start the transfer of another, older vRealize Automation deployment to your newly installed deployment.

Deployment Type
On the Deployment Type page, you decide which vRealize Automation components, and how many of each, you want to install.

Minimal
Minimal deployments use just one vRealize Automation appliance and one Windows server that hosts IaaS components. In minimal deployments, you may host the IaaS database on a separate SQL Server system, or install SQL on the IaaS Windows server.

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

Enterprise
Enterprise deployments involve multiple, separate appliances and Windows hosts, typically with load balancing. Enterprise deployments also permit you to host the IaaS database on a separate SQL Server system or on one of the IaaS Windows servers.

When you select an enterprise deployment, additional Installation Wizard pages appear in the summary list at the left of the wizard.

Infrastructure as a Service
The Infrastructure as a Service (IaaS) option selects whether or not to configure existing Windows machines with vRealize Automation modeling and provisioning capabilities.

When you select IaaS, additional Installation Wizard pages appear in the summary list at the left of the wizard.

Installation Prerequisites
On the Installation Prerequisites page, you pause to establish a connection to Windows machines that will host vRealize Automation IaaS. In addition, you select a time synchronization source.
IaaS Windows Servers

For a Windows machine to serve as an IaaS component host, you must download and install vCAC-IaaSManagementAgent-Setup.msi on the Windows machine.

Management Agent installation requires communication with a running vRealize Automation appliance. Each time that you install the Management Agent on Windows, that system becomes uniquely tied to the specific appliance and deployment.

Potential IaaS Windows servers that have the correct Management Agent installed appear under Discovered Hosts.

To have the Installation Wizard ignore a discovered host, click Delete. Deleting a Windows host does not remove its Management Agent. To uninstall the agent, use the Add or Remove Programs feature directly in Windows.

Time Source

You must synchronize every vRealize Automation appliance and IaaS Windows server to the same time source. The following sources are allowed:

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

Do not mix time sources within a vRealize Automation deployment.

vRealize Appliances

(Enterprise Deployments Only) On the vRealize Appliances page, you have the option to create a high-availability deployment with multiple vRealize Automation appliances.

Multiple appliances must be hosted behind a load balancer that you have separately installed. On a later wizard page, you verify and complete the configuration of the appliances and load balancer. For each vRealize Automation appliance that you add, enter its FQDN and root credentials.

Server Roles

(Enterprise Deployments Only) On the Server Roles page, you assign vRealize Automation IaaS component roles to the Windows machines where you had installed the Management Agent earlier.

IaaS Windows machines may serve as primary and additional Web servers, Manager Service hosts, DEM hosts, and Agent hosts. For more about IaaS component roles, see Infrastructure as a Service.

Separation of IaaS server roles is only possible in enterprise deployments. In minimal deployments, one Windows machine performs all roles.

Prerequisite Checker

On the Prerequisite Checker page, you check and fix your vRealize Automation Windows servers to support IaaS installation.
The prerequisite checker inspects Windows machines where you installed the Management Agent and will host IaaS components. Prerequisites include Java, Internet Information Services (IIS) settings, the Microsoft Distributed Transaction Coordinator (DTC) service, and more. For a detailed list of prerequisites, click **Show Details**.

The Installation Wizard allows you to proceed without checking for prerequisites, but be aware that installation might fail.

- To check for prerequisites, click **Run**.
- If prerequisites are missing, click **Show Details** to learn more, then click **Fix**.

  The Installation Wizard can fix most software or setting-based prerequisites. After making changes, the Installation Wizard restarts your IaaS hosts.
  
  The wizard cannot fix insufficient memory or CPU. You must correct those issues in vSphere or on your hardware, if they occur.

**vRealize Automation Host**

On the vRealize Automation Host page, you set the base URL address for vRealize Automation. The address is usually the vRealize Automation appliance or, in high availability deployments, a load balancer.

- When deploying only one vRealize Automation appliance with no load balancer, enter the vRealize Automation appliance FQDN. You can click to have the Installation Wizard populate the FQDN for you.
- When deploying an enterprise configuration that includes one or more vRealize Automation appliances behind load balancing, enter the load balancer FQDN instead.

  A single vRealize Automation appliance can still be deployed behind a load balancer. Taking that approach lets you add later appliances more easily, to expand the deployment.

**Single Sign On**

On the Single Sign On page, you set the vRealize Automation default tenant system administrator log in credentials.

The default tenant system administrator has the most permissions of any user, up to and including creating additional tenants. The default tenant system administrator credentials are separate from the vRealize Automation appliance root credentials.

**IaaS Host**

On the IaaS Host page, you set the base URL addresses for certain IaaS components. In addition, you create a security passphrase for the vRealize Automation IaaS SQL database.

**Minimal Deployments**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS Web Address</td>
<td>Enter the IaaS Windows server FQDN.</td>
</tr>
<tr>
<td>Install IaaS Components On</td>
<td>Select or enter the IaaS Windows server FQDN.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>
| **Security Passphrase** | Create a passphrase to encrypt data in the IaaS SQL database.  
- Record the passphrase, because you need it to restore the database if there is a failure or to add components after initial installation.  
- The passphrase cannot contain a double quotation mark (" ") character. |
| **Confirm Passphrase** | Re-enter the passphrase.                                                                                                                                                                             |

**Enterprise Deployments**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IaaS Web Address</strong></td>
<td>Enter the primary IaaS Web server FQDN. If deploying an enterprise configuration that includes load-balanced multiple IaaS Web servers, enter the load balancer FQDN instead.</td>
</tr>
<tr>
<td><strong>Manager Service Address</strong></td>
<td>Enter the primary Manager Service host FQDN. If deploying an enterprise configuration that includes load-balanced multiple Manager Service hosts, enter the load balancer FQDN instead.</td>
</tr>
</tbody>
</table>
| **Security Passphrase** | Create a passphrase to encrypt data in the IaaS SQL database.  
- Record the passphrase, because you need it to restore the database if there is a failure or to add components after initial installation.  
- The passphrase cannot contain a double quotation mark (" ") character. |
| **Confirm Passphrase** | Re-enter the passphrase.                                                                                                                                                                             |

**Microsoft SQL Server**

On the Microsoft SQL Server page, you configure the vRealize Automation IaaS SQL database. The IaaS database records provisioned machines, associated elements, and policies.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Server Name** | Enter the FQDN of the SQL Server host, which may be an IaaS Windows server or a separate server.  
If you need to specify a port number or named instance, use FQDN,Port\Instance format.  
When you use SQL AlwaysOn Availability Group (AAG) you specify the AAG listener FQDN. |
| **Database Name** | Accept the default of vra, or enter a different name for the IaaS database.                                                                 |
| **Create new database** | Allow the Installation Wizard to create the database.  
For this option to work, the account that runs the Management Agent on the primary IaaS Web server must have the sysadmin role in SQL. |
| **Use existing empty database** | Do not allow the Installation Wizard to create the database.  
When you separately create the database, the Windows user or SQL user credentials that you provide need dbo permission on the database. |
### Setting Description

**Default Settings**

(New Database Only) Clear this option only if you want to use an alternative storage location for IaaS data and log files. When cleared, enter directories for data (MDF) and logs. Your SQL Server service account must have write permission to the directories.

**Use SSL for database connection**

Encrypt connections to the database. To use this option, you must separately configure your SQL Server host for SSL. In addition, the IaaS Web server and Manager Service host must trust the SSL certificate from your SQL Server host.

**Windows Authentication**

Clear this option only if you want to use SQL authentication instead of Windows. When cleared, enter SQL authentication credentials.

**Installation Path**

Leave clear to accept the default of `%ProgramFiles(x86)\VMware`, or enter an alternative location.

- vRealize Automation files are not installed on the SQL Server host. They are placed on the primary IaaS Web server.
- If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.

### Web Role

(Enterprise Deployments Only) On the Web Role page, you separately configure the vRealize Automation IaaS Web site in IIS.

In an enterprise deployment, you separately specify the IaaS Windows machine that hosts the Web component. For high availability, multiple hosts are supported.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Name</td>
<td>Customize the name or leave it as the IIS Default Web Site. Avoid hosting additional Web sites in IIS. vRealize Automation sets the binding on its communication port to all unassigned IP addresses, making no additional bindings possible.</td>
</tr>
<tr>
<td>Port</td>
<td>Customize the port or accept the default of 443.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>Enter the FQDN of each IaaS Windows machine that hosts the IaaS Web component.</td>
</tr>
<tr>
<td>Username</td>
<td>In <code>DOMAIN\username</code> format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of <code>%ProgramFiles(x86)\VMware</code>, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
</tbody>
</table>

### Manager Service Role

(Enterprise Deployments Only) On the Manager Service Role page, you configure the separate vRealize Automation Windows machine that hosts the IaaS Manager Service.
In an enterprise deployment, you separately specify the host of the Manager Service, which is a Windows service. For high availability, multiple hosts are supported.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select the primary Manager Service host. Any additional hosts serve as backups to the primary.</td>
</tr>
<tr>
<td></td>
<td>When you install using the Installation Wizard, the service transparently fails over to a backup when a problem occurs. See About Automatic Manager Service Failover.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>Enter the FQDN of each IaaS Windows machine that hosts the Manager Service.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)\VMware, or enter an alternative location.</td>
</tr>
<tr>
<td></td>
<td>If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
</tbody>
</table>

**Distributed Execution Managers**

On the Distributed Execution Managers page, you configure the vRealize Automation Windows machines that host IaaS DEMs. Multiple DEM hosts are supported.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS Host Name</td>
<td>Enter the FQDN of each IaaS Windows machine that hosts a DEM.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>Enter a unique identifier for each DEM. All DEM names must be unique whether they are on the same or different hosts.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Instance Description</td>
<td>If needed, enter an explanation of the workflows associated with each DEM.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)\VMware, or enter an alternative location.</td>
</tr>
<tr>
<td></td>
<td>If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
</tbody>
</table>

**Agents**

On the Agents page, you create the linkage between vRealize Automation IaaS and the virtualization resources onto which infrastructure is deployed. You select an agent type, and complete the details for the corresponding endpoint.

- Multiple agents of the same or of different types are supported.
- You can install agents on the same or on separate servers.
- When on the same server, up to 25 agents of any type are supported.
When multiple agents of the same type are on the same server, each must have a unique name and different endpoint.

For high availability, you can install an agent of the same type, name, and endpoint on separate servers.

vSphere is usually one of the agent types.

You can add agents post-installation.

Agent Types

Table 1-20. vSphere

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select vSphere.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Enter a name for the vSphere endpoint.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)%\VMware, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

Table 1-21. EPI PowerShell

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select EpiPowerShell.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Type</td>
<td>From the drop-down, select what brand of provisioning the EPIserver endpoint is hosting.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the FQDN of the EPIserver.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)%\VMware, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
</tbody>
</table>
### Table 1-21. EPI PowerShell (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

### Table 1-22. HyperV

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select HyperV.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the login account to the HyperV endpoint instance.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)%\VMware, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

### Table 1-23. VDI PowerShell

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select VdiPowerShell.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Type</td>
<td>The endpoint type defaults to XenDesktop and cannot be changed.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the FQDN of the XenDesktop endpoint.</td>
</tr>
<tr>
<td>XenDesktop Version</td>
<td>From the drop-down, select the version.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)%\VMware, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>
### Table 1-24. Xen

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select Xen.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the login account to the Xen endpoint instance.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)\VMware, or enter an alternative location.</td>
</tr>
<tr>
<td></td>
<td>If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

### Table 1-25. WMI

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select WMI.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)\VMware, or enter an alternative location.</td>
</tr>
<tr>
<td></td>
<td>If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

### Table 1-26. Test

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>From the drop-down, select Test.</td>
</tr>
<tr>
<td>IaaS Host Name</td>
<td>From the drop-down, select the FQDN of the IaaS Windows machine that hosts the agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a unique identifier unless you are adding the same agent name and endpoint across separate servers for high availability.</td>
</tr>
</tbody>
</table>
Table 1-26. Test (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Path</td>
<td>Leave clear to accept the default of %ProgramFiles(x86)\VMware, or enter an alternative location. If you install multiple IaaS components on the same Windows machine, install them all under the same installation path.</td>
</tr>
<tr>
<td>Username</td>
<td>In DOMAIN\Username format, enter the service account. The account must be a domain account with local administrator privileges on the IaaS Windows server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
</tbody>
</table>

vRealize Appliance Certificate

On the vRealize Appliance Certificate page, you create or select the authentication certificate that the vRealize Automation appliance uses. When the certificate is self-signed, end users see and confirm it when they log in to vRealize Automation in a browser.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Action</td>
<td>Keep Existing Use the certificate already on this vRealize Automation appliance. Verify the details in the entries below, such as the serial number and fingerprint.</td>
</tr>
<tr>
<td>Generate Certificate</td>
<td>Use the wizard to generate a vRealize Automation appliance self-signed certificate.</td>
</tr>
</tbody>
</table>
| Generate Signing Request | Create a certificate signing request (CSR) file for your certificate authority (CA). A CSR helps your CA create a certificate with the correct values for you to import.  
1 Enter Organization, Organizational Unit, and Country Code (see below).  
2 Click Generate Signing Request.  
3 To download the CSR file for your CA, click the link that appears. |
| Import                | Identify a PEM format certificate file, have the wizard add it to the correct store, and load it for use by vRealize Automation. Unless you are importing a certificate created from your CSR, this option requires you to enter the certificate private key, private key passphrase (if any), and certificate chain. When importing a CA-provided PEM that was created from your CSR, leave the private key and passphrase blank. |
| Common Name           | The FQDN of the vRealize Automation appliance. In high-availability enterprise deployments with a load balancer in front of multiple appliances, this entry is the load balancer FQDN instead. |
| Organization          | Enter text to represent your larger department or business unit.                                                                                  |
| Organizational Unit   | Enter text to represent your smaller department or workgroup.                                                                                     |
| Country Code          | Enter an abbreviation for your country of operation.                                                                                             |
| Serial                | Unique alphanumeric identifier                                                                                                                   |
### Setting | Description
--- | ---
Fingerprint | Unique alphanumeric string used for identifying a certificate or comparing one against another
Valid Since | Timestamp after which the certificate can be used
Valid To | Timestamp after which the certificate can no longer be used

### Web Certificate

On the Web Certificate page, you create or select the authentication certificate that the IaaS Web server uses. The vRealize Automation appliance connects to the Web server and needs to authenticate and trust it.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Action</td>
<td><strong>Keep Existing</strong> Use the certificate already on this IaaS Web server. Verify the details in the entries below, such as the serial number and fingerprint.</td>
</tr>
<tr>
<td></td>
<td><strong>Generate Certificate</strong> Use the wizard to generate an IaaS Web server self-signed certificate.</td>
</tr>
</tbody>
</table>
| | **Generate Signing Request** Create a certificate signing request (CSR) file for your certificate authority (CA). A CSR helps your CA create a certificate with the correct values for you to import.  
  1. Enter Organization, Organizational Unit, and Country Code (see below).  
  2. Click **Generate Signing Request**.  
  3. To download the CSR file for your CA, click the link that appears. |
| | **Import** Identify a PEM format certificate file, have the wizard add it to the correct store, and load it for use by vRealize Automation.  
  Unless you are importing a certificate created from your CSR, this option requires you to enter the certificate private key, private key passphrase (if any), and certificate chain.  
  When importing a CA-provided PEM that was created from your CSR, leave the private key and passphrase blank. |
| | **Provide Certificate Thumbprint** Load a certificate that you already added to the correct store. |
| Common Name | The FQDN of the IaaS Web server.  
  In high-availability enterprise deployments with a load balancer in front of multiple Web servers, this entry is the load balancer FQDN instead. |
| Organization | Enter text to represent your larger department or business unit. |
| Organizational Unit | Enter text to represent your smaller department or workgroup. |
| Country Code | Enter an abbreviation for your country of operation. |
| Serial | Unique alphanumeric identifier |
| Fingerprint | Unique alphanumeric string used for identifying a certificate or comparing one against another |
Manager Service Certificate

(Enterprise Deployments Only) On the Manager Service Certificate page, you create or select the authentication certificate that the vRealize Automation IaaS Manager Service host uses. The other IaaS Windows servers connect to the Manager Service host and need to authenticate and trust it.

This page appears only when you host the Manager Service on a separate machine from the IaaS Web server. When they are hosted on the same machine, the Web certificate provides authentication for both roles.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Since</td>
<td>Timestamp after which the certificate can be used</td>
</tr>
<tr>
<td>Valid To</td>
<td>Timestamp after which the certificate can no longer be used</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Certificate Action            | Keep Existing
Use the certificate already on this IaaS Manager Service host. Verify the details in the entries below, such as the serial number and fingerprint. |
| Generate Certificate          | Use the wizard to generate an IaaS Manager Service host self-signed certificate. |
| Generate Signing Request      | Create a certificate signing request (CSR) file for your certificate authority (CA). A CSR helps your CA create a certificate with the correct values for you to import.  
   1. Enter Organization, Organizational Unit, and Country Code (see below).  
   2. Click Generate Signing Request.  
   3. To download the CSR file for your CA, click the link that appears. |
<p>| Import                        | Identify a PEM format certificate file, have the wizard add it to the correct store, and load it for use by vRealize Automation. Unless you are importing a certificate created from your CSR, this option requires you to enter the certificate private key, private key passphrase (if any), and certificate chain. When importing a CA-provided PEM that was created from your CSR, leave the private key and passphrase blank. |
| Provide Certificate Thumbprint| Load a certificate that you already added to the correct store.               |
| Common Name                  | The FQDN of the IaaS Manager Service host.                                  |
| Organization                 | Enter text to represent your larger department or business unit.            |
| Organizational Unit          | Enter text to represent your smaller department or workgroup.               |
| Country Code                 | Enter an abbreviation for your country of operation.                       |
| Serial                       | Unique alphanumeric identifier.                                            |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Unique alphanumeric string used for identifying a certificate or comparing one against another</td>
</tr>
<tr>
<td>Valid Since</td>
<td>Timestamp after which the certificate can be used</td>
</tr>
<tr>
<td>Valid To</td>
<td>Timestamp after which the certificate can no longer be used</td>
</tr>
</tbody>
</table>

**Load Balancers**

(Enterprise Deployments Only) On the Load Balancers page, you pause to configure load balancers for the correct pool of vRealize Automation member systems.

The load balancers list is informational only. Based on your earlier wizard entries, it presents each load balancer in your deployment along with members, their component role, FQDN, and port number.

Pause here, and use the list while you log in to your load balancers to add vRealize Automation members and open ports.

**Validation**

On the Validation page, you verify that vRealize Automation installation can proceed.

To check that all vRealize Automation components, roles, and accounts are correct and that systems can authenticate with one another, click **Validate**. The process can take up to a half hour or more depending on your environment.

If errors occur, expand the failed line item and make corrections based on the status and messages presented. You cannot proceed with vRealize Automation installation until validation passes.

**Create Snapshots**

On the Create Snapshots page, you pause to take virtual machine snapshots of all vRealize Automation components before proceeding with installation.

Even though validation has passed, you are strongly advised to prepare for any unexpected issues around installation. Before starting the installation, use your vSphere client to take a snapshot of every vRealize Automation appliance and IaaS Windows server. Otherwise, you have to re-enter all of the wizard settings to get back to this point.

If you have enough resources, you can take snapshots of virtual machines that are running. A better practice is to stop them first.

1. At the upper right of the Installation Wizard, click **Logout**.

   **Important** If you close the wizard using anything other than **Logout**, you will not be able to reopen the wizard.

2. In vSphere, shut down the guest operating system of every vRealize Automation appliance and IaaS Windows server.

3. Right-click the virtual machines, and select **Take Snapshot**.

4. Name the snapshot.
5 To include machine memory in the snapshot, select **Snapshot the virtual machine memory**.

6 Click **OK**.
   
   Wait for the snapshots to be created.

7 Power on the guest operating system of every vRealize Automation appliance and IaaS Windows server.

8 Return to the Installation Wizard snapshot page by logging in again as root.
   
   https://vrealize-automation-appliance-FQDN:5480

**Installation Details**

On the Installation Details page, you start the vRealize Automation installation or retry it if problems occurred.

To start installation, click **Install**. Depending on your environment, installation can take up to an hour or more.

During or after installation, you can click the **Collect Logs** button.

- When you collect logs, a ZIP file download link appears above the status table.
- When you collect logs more than once, each collection overwrites the previous one.
   
   If you want the current logs, download them before clicking **Collect Logs** again.

If problems occur, the wizard stops the installation and displays messages to help you make corrections. After evaluating the messages and noting the corrections you need, you might or might not need the snapshots you created.

**Do Not Revert to Snapshots**

If the wizard enables **Retry Failed**, you may make corrections and retry the installation without reverting any machines to snapshots.

After making corrections, click **Retry Failed**.

**Revert IaaS Windows Servers to Snapshots**

If the wizard enables **Retry All IaaS**, take the following steps.

1 In vSphere, revert all IaaS Windows machines to the snapshots taken on the previous wizard page.

2 If the snapshots were taken after a shut down, power on guest operating systems.

3 If you used an external SQL Server, delete the vRealize Automation SQL database.

4 Make corrections.

5 Click **Retry All IaaS**.
Revert Appliances and IaaS Windows Servers to Snapshots

If the wizard displays messages about the vRealize Automation appliance, take the following steps.

1. In vSphere, revert all vRealize Automation appliances and IaaS Windows machines to the snapshots taken on the previous wizard page.
2. If the snapshots were taken after a shut down, power on guest operating systems.
3. If you used an external SQL Server, delete the vRealize Automation SQL database.
5. Return to the Installation Wizard by logging in again as root.
   https://vrealize-automation-appliance-FQDN:5480
6. Return to the Installation Details page, and click Install.

Licensing

On the Licensing page, you enter a key to activate the installed vRealize Automation product.

In New License Key, enter your key, and click Submit Key. You can separately submit more than one key, including keys for standalone vRealize Automation, vRealize Suite, vRealize Business for Cloud, and vRealize Code Stream.

On this page you also select whether to enable vRealize Code Stream. vRealize Code Stream is not supported for high-availability or production vRealize Automation deployments, and requires the vRealize Code Stream Management Pack. For more information, see Licensing vRealize Code Stream.

Telemetry

On the Telemetry page, you decide whether or not vRealize Automation sends usage statistics to VMware as part of the Customer Experience Improvement Program.

Select or clear the option to join the Customer Experience Improvement Program (CEIP).

For more information, see The Customer Experience Improvement Program.

Post Installation Options

On the Post Installation Options page, you have options for creating new vRealize Automation data or migrating older deployment data to your new installation.

- Configure Initial Content creates a new, local user of the default tenant. That local user can start the configuration process in the default tenant.
  
  For this option, you must have added at least one vSphere endpoint earlier, on the Agents page of the Installation Wizard.

- Migrate a Deployment transfers your older vRealize Automation data to this newly installed deployment. Migration preserves essential elements such as groups, blueprints, and endpoints.

- Continue takes you to the end of the Installation Wizard.
Initial Content Configuration

On the Initial Content Configuration page, you create a new, local vRealize Automation default tenant user who can begin a content workflow for a vSphere endpoint.

**Note**  This option is only available if you had added at least one vSphere endpoint earlier, on the Agents page.

The new, local username is configurationadmin. vRealize Automation grants configurationadmin the following privileges.

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

Enter and confirm a login password for configurationadmin. To generate a catalog item so that configurationadmin can start the configuration process after logging in to the default tenant, click **Create Initial Content**.

Migration Configuration

On the Migration Configuration page, you can start the transfer of another, older vRealize Automation deployment to your newly installed deployment.

Before migrating an older deployment, address the following guidelines.

- Thoroughly review the vRealize Automation migration guide associated with your older deployment version. Prerequisites and other details might vary.
- Migrate the older tenants and identity stores to VMware Identity Manager on the new deployment.
- Clone the older IaaS SQL Server database and restore it to the new deployment IaaS database. Note the name of the cloned database.
- Obtain and make note of the encryption key for the older IaaS SQL Server database.
- Create and make note of a new passphrase for re-encrypting the migrated data.
- Note the older vRealize Automation appliance or load balancer FQDN and root login credentials.
- Note the new deployment root login credentials.

The Standard vRealize Automation Installation Interfaces

After running the Installation Wizard, you might need or want to perform certain installation tasks manually, through the standard interfaces.
The Installation Wizard described in Installing vRealize Automation with the Installation Wizard is your primary tool for new vRealize Automation installations. However, after you run the wizard, some operations still require the older, manual installation process.

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

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

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

**Using the Standard Interfaces for Minimal Deployments**

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

**Minimal Deployment Checklist**

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

Complete the high-level tasks in the following order.

**Table 1-27. Minimal Deployment Checklist**

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

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

Prerequisites

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

Procedure

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

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

   Continue past any certificate warnings.

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Time</td>
<td>Synchronize to the vRealize Automation appliance ESXi host.</td>
</tr>
<tr>
<td>Time Server</td>
<td>Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.</td>
</tr>
</tbody>
</table>

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

4. Select vRA Settings > Host Settings.

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

   **Note**  Configure SSO settings as described later in this procedure whenever you use Update Host to set the host name.
5 Select the certificate type from the **Certificate Action** menu.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Existing</td>
<td>Leave the current SSL configuration. Select this option to cancel your changes.</td>
</tr>
</tbody>
</table>
| Generate Certificate | a The value displayed in the **Common Name** text box is the Host Name as it appears on the upper part of the page. If any additional instances of the vRealize Automation appliance available, their FQDNs are included in the SAN attribute of the certificate.  
   b Enter your organization name, such as your company name, in the **Organization** text box.  
   c Enter your organizational unit, such as your department name or location, in the **Organizational Unit** text box.  
   d Enter a two-letter ISO 3166 country code, such as **US**, in the **Country** text box. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Generate Signing Request | a  Select Generate Signing Request.  
 b  Review the entries in the Organization, Organization Unit, Country Code, and Common Name text boxes. These entries are populated from the existing certificate. You can edit these entries if needed.  
 c  Click Generate CSR to generate a certificate signing request, and then click the Download the generated CSR here link to open a dialog that enables you to save the CSR to a location where you can send it to a certificate authority.  
 d  When you receive the prepared certificate, click Import and follow instructions for importing a certificate into vRealize Automation. |
| Import                 | a  Copy the certificate values from BEGIN PRIVATE KEY to END PRIVATE KEY, including the header and footer, and paste them in the RSA Private Key text box.  
 b  Copy the certificate values from BEGIN CERTIFICATE to END CERTIFICATE, including the header and footer, and paste them in the Certificate Chain text box. For multiple certificate values, include a BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate.  
 Note  In the case of chained certificates, additional attributes may be available.  
 c  (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the Passphrase text box. |

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

7  Configure the SSO settings.

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

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

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

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

10 Click Services and verify that services are registered.

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

Note  You can log in to the appliance and run tail -f /var/log/vcac/catalina.out to monitor startup of the services.
11 Enter your license information.
   a Click vRA Settings > Licensing.
   b Click Licensing.
   c Enter a valid vRealize Automation license key that you downloaded when you downloaded the installation files, and click Submit Key.

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

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

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

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

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

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

**What to do next**

See Install the Infrastructure Components.

**Installing IaaS Components**

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

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

**Enable Time Synchronization on the Windows Server**

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

**Procedure**

1. Open a command prompt on the Windows installation machine.
2. Type the following command to navigate to the VMware Tools directory.
   ```
   cd C:\Program Files\VMware\VMware Tools
   ```
3. Type the command to display the timesync status.
   ```
   VMwareToolboxCmd.exe timesync status
   ```
4. If timesync is disabled, type the following command to enable it.
   ```
   VMwareToolboxCmd.exe timesync enable
   ```

**IaaS Certificates**

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

In a distributed environment, obtain a domain certificate from a trusted certificate authority. For information about installing domain certificates for IaaS components, see Install IaaS Certificates in the distributed deployment chapter.

**Install the Infrastructure Components**

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

**Prerequisites**

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

**Procedure**

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

2. Select the Installation Type
   
   The system administrator runs the installer wizard from the Windows 2008 or 2012 installation machine.
3 **Check Prerequisites**
   The Prerequisite Checker verifies that your machine meets IaaS installation requirements.

4 **Specify Server and Account Settings**
   The vRealize Automation system administrator specifies server and account settings for the Windows installation server and selects a SQL database server instance and authentication method.

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

6 **Register the IaaS Components**
   The system administrator installs the IaaS certificate and registers the IaaS components with the SSO.

7 **Finish the Installation**
   The system administrator finishes the IaaS installation.

**Download the vRealize Automation IaaS Installer**

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

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

**Prerequisites**

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

**Procedure**

1. Log in to the IaaS Windows server using an account that has administrator rights.
2. Open a Web browser directly to the vRealize Automation appliance installer URL.
   
   `https://vrealize-automation-appliance-FQDN:5480/installer`

3. Click **IaaS Installer**.
4. Save `setup__vrealize-automation-appliance-FQDN@5480` to the Windows server.
   
   Do not change the installer file name. It is used to connect the installation to the vRealize Automation appliance.

**Select the Installation Type**

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

**Prerequisites**

- Download the vRealize Automation IaaS Installer.
Procedure

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

2 Click Next.

3 Accept the license agreement and click Next.

4 On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a Type the user name, which is root, and the password.
      The password is the password that you specified when you deployed the vRealize Automation appliance.
   b Select Accept Certificate.
   c Click View Certificate.
      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5 Select Accept Certificate.

6 Click Next.

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

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

Prerequisites
Select the Installation Type.

Procedure

1 Complete the Prerequisite Check.

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

2 Click Next.

The machine meets installation requirements.
Specify Server and Account Settings

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

Prerequisites

Check Prerequisites.

Procedure

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

2. Type a phrase in the Passphrase text box.

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

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

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

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

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

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

5. Select the authentication method.

   - Select **Use Windows authentication** if you want to create the database using the Windows credentials of the current user. The user must have SQL sys_admin privileges.

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

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

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

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

7. Click **Next**.

Specify Managers and Agents

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

Specify Server and Account Settings.

**Procedure**

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

2. Accept the default to install a vSphere agent to enable provisioning with vSphere or deselect it if applicable.
   a. Select **Install and configure vSphere agent**.
   b. Accept the default agent and endpoint, or type a name.

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

3. Click **Next**.

**Register the IaaS Components**

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

**Prerequisites**

Download the vRealize Automation IaaS Installer.

**Procedure**

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

   If you have multiple virtual appliances and are using a load balancer, enter the load balancer virtual appliance path.

2. Click **Load** to populate the value of **SSO Default Tenant** (vsphere.local).

3. Click **Download** to retrieve the certificate from the vRealize Automation appliance.

   You can click **View Certificate** to view the certificate details.

4. Select **Accept Certificate** to install the SSO certificate.

5. In the SSO Administrator panel, type **administrator** in the **User name** text box and the password you defined for this user when you configured SSO in **Password** and **Confirm password**.

6. Click the test link to the right of the **User name** field to validate the entered password.

7. Accept the default in **IaaS Server**, which contains the host name of the Windows machine where you are installing.

8. Click the test link to the right of the **IaaS Server** field to validate connectivity.
9 Click **Next**.

If any errors appear after you click **Next**, resolve them before proceeding.

### Finish the Installation

The system administrator finishes the IaaS installation.

### Prerequisites

- Register the IaaS Components.
- Verify that machine on which you are installing is connected to the network and is able to connect to the vRealize Automation appliance from which you download the IaaS installer.

### Procedure

1. Review the information on the **Ready to Install** page and click **Install**.

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

2. When the success message appears, leave the **Guide me through initial configuration** check box selected and click **Next**, and **Finish**.

3. Close the **Configure the System** message box.

The installation is now finished.

### What to do next

**Verify IaaS Services.**

### Using the Standard Interfaces for Distributed Deployments

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

### Distributed Deployment Checklist

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

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

### Table 1-28. Distributed Deployment Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴 Plan and prepare the installation environment and verify that all installation prerequisites are met.</td>
<td>Preparing for vRealize Automation Installation</td>
</tr>
<tr>
<td>🔴 Plan for and obtain your SSL certificates.</td>
<td>Certificate Trust Requirements in a Distributed Deployment</td>
</tr>
</tbody>
</table>
**Table 1-28. Distributed Deployment Checklist (Continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy the lead vRealize Automation appliance server, and any additional appliances you require for redundancy and high availability.</td>
<td>Deploy the vRealize Automation Appliance</td>
</tr>
<tr>
<td>Configure your load balancer to handle vRealize Automation appliance traffic.</td>
<td>Configuring Your Load Balancer</td>
</tr>
<tr>
<td>Configure the lead vRealize Automation appliance server, and any additional appliances you deployed for redundancy and high availability.</td>
<td>Configuring Appliances for vRealize Automation</td>
</tr>
<tr>
<td>Configure your load balancer to handle the vRealize Automation IaaS component traffic and install vRealize Automation IaaS components.</td>
<td>Install the IaaS Components in a Distributed Configuration</td>
</tr>
<tr>
<td>If required, install agents to integrate with external systems.</td>
<td>Installing vRealize Automation Agents</td>
</tr>
<tr>
<td>Configure the default tenant and provide the IaaS license.</td>
<td>Configure Access to the Default Tenant</td>
</tr>
</tbody>
</table>

**vRealize Orchestrator**

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

For information about connecting vRealize Automation and vRealize Orchestrator, see VMware vRealize Orchestrator Plug-In for vRealize Automation.

**Directories Management**

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

**Disabling Load Balancer Health Checks**

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

For workload distribution and failover, you can place multiple vRealize Automation appliances behind a load balancer. In addition, you can place multiple IaaS Web servers and multiple IaaS Manager Service servers behind their respective load balancers.
When using load balancers, do not allow the load balancers to send health checks at any time during installation. Health checks might interfere with installation or cause the installation to behave unpredictably.

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

Certificate Trust Requirements in a Distributed Deployment

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

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

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

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

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

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

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

If you are need to update system generated self-signed certificates with user or CA supplied certificates, see Updating vRealize Automation Certificates.

The Certificate Trust Requirements table summarizes the trust registration requirements for various imported certificates.
### Table 1-29. Certificate Trust Requirements

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

### Configure Web Component, Manager Service and DEM Host Certificate Trust

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

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

**Prerequisites**

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

**Procedure**

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

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

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

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

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

**What to do next**

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

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

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

Table 1-30. vRealize Automation Appliance

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

Table 1-31. IaaS Windows Servers

<table>
<thead>
<tr>
<th>Variable</th>
<th>My Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IaaS Web Server with Model Manager Data FQDN</td>
<td>web.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>Primary IaaS Web Server with Model Manager Data IP address</td>
<td>123.234.1.107</td>
<td></td>
</tr>
<tr>
<td>For reference only; do not enter IP addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional IaaS Web Server FQDN</td>
<td></td>
<td>web2.mycompany.com</td>
</tr>
</tbody>
</table>
### Table 1-31. IaaS Windows Servers (Continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>My Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional IaaS Web Server IP address</td>
<td>For reference only; do not enter IP addresses</td>
<td>123.234.1.108</td>
</tr>
<tr>
<td>IaaS Web Server load balancer FQDN</td>
<td>web-balance.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>IaaS Web Server load balancer IP address</td>
<td>For reference only; do not enter IP addresses</td>
<td>123.234.1.202</td>
</tr>
<tr>
<td>Active IaaS Manager Service host FQDN</td>
<td>mgr-svc.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>Active IaaS Manager Service host IP address</td>
<td>For reference only; do not enter IP addresses</td>
<td>123.234.1.109</td>
</tr>
<tr>
<td>Passive IaaS Manager Service host FQDN</td>
<td>mgr-svc2.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>Passive IaaS Manager Service host IP address</td>
<td>For reference only; do not enter IP addresses</td>
<td>123.234.1.110</td>
</tr>
<tr>
<td>IaaS Manager Service host load balancer FQDN</td>
<td>mgr-svc-balance.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>IaaS Manager Service host load balancer IP address</td>
<td>For reference only; do not enter IP addresses</td>
<td>123.234.203</td>
</tr>
<tr>
<td>For IaaS services, domain account with administrator rights on hosts</td>
<td>SUPPORT\provisioner</td>
<td></td>
</tr>
<tr>
<td>Account password</td>
<td></td>
<td>login123</td>
</tr>
</tbody>
</table>

### Table 1-32. IaaS SQL Server Database

<table>
<thead>
<tr>
<th>Variable</th>
<th>My Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database instance</td>
<td></td>
<td>IAASSQL</td>
</tr>
<tr>
<td>Database name</td>
<td>vCAC (default)</td>
<td>vCAC</td>
</tr>
<tr>
<td>Passphrase (used at installation, upgrade, and migration)</td>
<td></td>
<td>login123</td>
</tr>
</tbody>
</table>
Table 1-33. IaaS Distributed Execution Managers

<table>
<thead>
<tr>
<th>Variable</th>
<th>My Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM host FQDN</td>
<td>dem.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>DEM host IP address</td>
<td>123.234.1.111</td>
<td></td>
</tr>
<tr>
<td>For reference only; do not enter IP addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEM host FQDN</td>
<td>dem2.mycompany.com</td>
<td></td>
</tr>
<tr>
<td>DEM host IP address</td>
<td>123.234.1.112</td>
<td></td>
</tr>
<tr>
<td>For reference only; do not enter IP addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unique DEM Orchestrator name</td>
<td>Orchestrator-1</td>
<td></td>
</tr>
<tr>
<td>Unique DEM Orchestrator name</td>
<td>Orchestrator-2</td>
<td></td>
</tr>
<tr>
<td>Unique DEM Worker name</td>
<td>Worker-1</td>
<td></td>
</tr>
<tr>
<td>Unique DEM Worker name</td>
<td>Worker-2</td>
<td></td>
</tr>
<tr>
<td>Unique DEM Worker name</td>
<td>Worker-3</td>
<td></td>
</tr>
<tr>
<td>Unique DEM Worker name</td>
<td>Worker-4</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Your Load Balancer

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

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

1. Install your load balancer.
2. Enable session affinity, also known as sticky sessions.
3. Ensure that the timeout on the load balancer is at least 100 seconds.
4. If your network or load balancer requires it, import a certificate to your load balancer. For information about trust relationships and certificates, see Certificate Trust Requirements in a Distributed Deployment. For information about extracting certificates, see Extracting Certificates and Private Keys.
5. Configure the load balancer for vRealize Automation appliance traffic.

Note When you set up virtual appliances under the load balancer, do so only for virtual appliances that have been configured for use with vRealize Automation. If unconfigured appliances are set up, you see fault responses.
For more about load balancers, see vRealize Automation Load Balancing.

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

Configuring Appliances for vRealize Automation

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

Configure the First vRealize Automation Appliance in a Cluster

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

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Obtain an authentication certificate for the vRealize Automation appliance.
  
  If your network or load balancer requires it, later procedures copy the certificate to the load balancer and additional appliances.

Procedure

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

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

   Continue past any certificate warnings.

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Time</td>
<td>Synchronize to the vRealize Automation appliance ESXi host.</td>
</tr>
<tr>
<td>Time Server</td>
<td>Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.</td>
</tr>
</tbody>
</table>

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

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

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

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

If you are using a PEM-encoded certificate, for example for a distributed environment, select **Import**. Certificates that you import must be trusted and must also be applicable to all instances of vRealize Automation appliance and any load balancer through the use of Subject Alternative Name (SAN) certificates.

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

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

a  Client/server certificate signed by the intermediate CA certificate

b  One or more intermediate certificates

c  A root CA certificate

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Existing</td>
<td>Leave the current SSL configuration. Select this option to cancel your changes.</td>
</tr>
</tbody>
</table>
| Generate Certificate | a  The value displayed in the **Common Name** text box is the Host Name as it appears on the upper part of the page. If any additional instances of the vRealize Automation appliance available, their FQDNs are included in the SAN attribute of the certificate.  
   b  Enter your organization name, such as your company name, in the **Organization** text box.  
   c  Enter your organizational unit, such as your department name or location, in the **Organizational Unit** text box.  
   d  Enter a two-letter ISO 3166 country code, such as *US*, in the **Country** text box. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate Signing Request</td>
<td>a Select <strong>Generate Signing Request</strong>.</td>
</tr>
<tr>
<td></td>
<td>b Review the entries in the <strong>Organization</strong>, <strong>Organization Unit</strong>, <strong>Country Code</strong>, and <strong>Common Name</strong> text boxes. These entries are populated from the existing certificate. You can edit these entries if needed.</td>
</tr>
<tr>
<td></td>
<td>c Click <strong>Generate CSR</strong> to generate a certificate signing request, and then click the <strong>Download the generated CSR here</strong> link to open a dialog that enables you to save the CSR to a location where you can send it to a certificate authority.</td>
</tr>
<tr>
<td></td>
<td>d When you receive the prepared certificate, click <strong>Import</strong> and follow instructions for importing a certificate into vRealize Automation.</td>
</tr>
<tr>
<td>Import</td>
<td>a Copy the certificate values from BEGIN PRIVATE KEY to END PRIVATE KEY, including the header and footer, and paste them in the <strong>RSA Private Key</strong> text box.</td>
</tr>
<tr>
<td></td>
<td>b Copy the certificate values from BEGIN CERTIFICATE to END CERTIFICATE, including the header and footer, and paste them in the <strong>Certificate Chain</strong> text box. For multiple certificate values, include a BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In the case of chained certificates, additional attributes may be available.</td>
</tr>
<tr>
<td></td>
<td>c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the <strong>Passphrase</strong> text box.</td>
</tr>
</tbody>
</table>

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

7 If required by your network or load balancer, copy the imported or newly created certificate to the virtual appliance load balancer.
   You might need to enable root SSH access in order to export the certificate.
   a If not already logged in, log in to the vRealize Automation appliance Management Console as root.
   b Click the **Admin** tab.
   c Click the **Admin** sub menu.
   d Select the **SSH service enabled** check box.
      Deselect the check box to disable SSH when finished.
   e Select the **Administrator SSH login** check box.
      Deselect the check box to disable SSH when finished.
   f Click **Save Settings**.

8 Configure the SSO settings.
9 Click Services.

All services must be running before you can install a license or log in to the console. They usually start in about 10 minutes.

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

10 Enter your license information.

a Click vRA Settings > Licensing.

b Click Licensing.

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

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

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

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

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

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

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

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

14 Click Save Settings.

15 Confirm that you can log in to vRealize Automation.

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

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

b If prompted, continue past the certificate warnings.

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

The interface opens to the Tenants page on the Administration tab. A single tenant named vsphere.local appears in the list.
Configuring Additional Instances of the vRealize Automation Appliance

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

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

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

Add Another vRealize Automation Appliance to the Cluster

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

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

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

Prerequisites

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

Procedure

1. Log in to the new vRealize Automation appliance management interface as root.
   https://vrealize-automation-appliance-FQDN:5480
   Continue past any certificate warnings.
2. If the installation wizard appears, cancel it so that you can go to the management interface instead of the wizard.
3. Select Admin > Time Settings, and set the time source to the same one that the rest of the cluster appliances use.
4 Select vRA Settings > Cluster.

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

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

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

7 Click **Join Cluster**.

8 Continue past any certificate warnings.

   Services for the cluster are restarted.

9 Verify that services are running.

   a Click the **Services** tab.

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

**Disable Unused Services**

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

**Prerequisites**

**Add Another vRealize Automation Appliance to the Cluster**

**Procedure**

1 Log in to the vRealize Automation appliance console.

2 Stop the vRealize Orchestrator service.

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

**Validate the Distributed Deployment**

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

**Procedure**

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

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

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

3 After verifying that you can access the new vRealize Automation appliance through the load balancer, re-enable the other nodes.
Install the IaaS Components in a Distributed Configuration

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

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

Prerequisites

- Configure the First vRealize Automation Appliance in a Cluster.
- If your site includes multiple vRealize Automation appliances, Add Another vRealize Automation Appliance to the Cluster.
- Verify that the server meets the requirements in IaaS Windows Servers.
- Obtain a certificate from a trusted certificate authority for import to the trusted root certificate store of the machines on which you intend to install the Component Website and Model Manager data.
- If you are using load balancers in your environment, verify that they meet the configuration requirements.

Procedure

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

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

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

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

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

6. Install the Active Manager Service
   The active Manager Service is a Windows service that coordinates communication between IaaS Distributed Execution Managers, the database, agents, proxy agents, and SMTP.
7 Install a Backup Manager Service Component
   The backup Manager Service provides redundancy and high availability, and may be started manually if the active service stops.

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

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

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

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

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

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

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

7 Verify that the certificate and its chain is trusted.

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

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

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

**What to do next**

**Download the vRealize Automation IaaS Installer.**

**Download the vRealize Automation IaaS Installer**

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

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

**Prerequisites**

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

**Procedure**

1 (Optional) Activate HTTP if you are installing on a Windows 2012 machine.
   a Select **Features > Add Features** from Server Manager.
   b Expand **WCF Services** under .NET Framework Features.
   c Select **HTTP Activation**.

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

3 Open a Web browser directly to the vRealize Automation appliance installer URL. Do not use a load balancer address.
   https://vrealize-automation-appliance-FQDN:5480/installer

4 Click **IaaS Installer**.
5 Save setup\_vrealize-automation-appliance-FQDN@5480 to the Windows server.

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

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

What to do next

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

Choosing an IaaS Database Scenario

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

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

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

Table 1-34. Choosing an IaaS Database Scenario

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the IaaS database manually using the provided database scripts. This option enables a database administrator to review the changes carefully before creating the database.</td>
<td>Create the IaaS Database Manually.</td>
</tr>
<tr>
<td>Prepare an empty database and use the installer to populate the database schema. This option enables the installer to use a database user with dbo privileges to populate the database.</td>
<td>Prepare an Empty Database.</td>
</tr>
<tr>
<td>Use the installer to create the database. This is the simplest option but requires the use of sysadmin privileges in the installer.</td>
<td>Create the IaaS Database Using the Installation Wizard.</td>
</tr>
</tbody>
</table>

Create the IaaS Database Manually

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

Prerequisites

- Install Microsoft .NET Framework 4.5.2 or later on the SQL Server host.
- Use Windows Authentication, rather than SQL Authentication, to connect to the database.
- Verify the database installation prerequisites. See IaaS SQL Server Host.
Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.

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

Procedure

1. Navigate to the Database subdirectory in the directory where you extracted the installation zip archive.

2. Extract the DBInstall.zip archive to a local directory.

3. Log in to the Windows database host with sufficient rights to create and drop databases sysadmin privileges in the SQL Server instance.

4. Review the database deployment scripts as needed. In particular, review the settings in the DBSettings section of CreateDatabase.sql and edit them if necessary. The settings in the script are the recommended settings. Only ALLOW_SNAPSHOT_ISOLATION ON and READ_COMMITTED_SNAPSHOT ON are required.

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

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

Table 1-35. Database Values

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

What to do next

Install the IaaS Components in a Distributed Configuration.

Prepare an Empty Database

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

Prerequisites

- Verify the database installation prerequisites. See IaaS SQL Server Host.
- Open a Web browser to the vRealize Automation appliance installer URL, and download the IaaS database installation scripts.
  
  https://vrealize-automation-appliance-FQDN:5480/installer

Procedure

1. Navigate to the Database directory within the directory where you extracted the installation zip archive.

2. Extract the DBInstall.zip archive to a local directory.

3. Log in to the Windows database host with sysadmin privileges within the SQL Server instance.

4. Edit the following files, and replace all instances of the variables in the table with the correct values for your environment.

   CreateDatabase.sql
   SetDatabaseSettings.sql

   **Table 1-36. Database Values**

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

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

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

6. Open SQL Server Management Studio.
7 Click **New Query**.
   
   An SQL Query window opens.

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

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

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

11 Click **Execute**.

   The script runs and creates the database.

**What to do next**

Install the IaaS Components in a Distributed Configuration.

**Create the IaaS Database Using the Installation Wizard**

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

The following steps describe how to create the IaaS database using the installer or populate an existing empty database. It is also possible to create the database manually. See Create the IaaS Database Manually.

**Prerequisites**

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

- Download the vRealize Automation IaaS Installer.

**Procedure**

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

2 Click **Next**.

3 Accept the license agreement and click **Next**.
4  On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a  Type the user name, which is root, and the password.
      The password is the password that you specified when you deployed the vRealize Automation appliance.
   b  Select Accept Certificate.
   c  Click View Certificate.
      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance.
      You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.
5  Click Next.
6  Select Custom Install on the Installation Type page.
7  Select IaaS Server under Component Selection on the Installation Type page.
8  Accept the root install location or click Change and select an installation path.
    Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
    If you install more than one IaaS component, always install them to the same path.
9  Click Next.
10 On the IaaS Server Custom Install page, select Database.
11 In the Database Instance text box, specify the database instance or click Scan and select from the list of instances. If the database instance is on a non-default port, include the port number in instance specification by using the form dbhost,SQL_port_number\SQLinstance. The Microsoft SQL default port number is 1443.
12 (Optional) Select the Use SSL for database connection checkbox.
    By default, the checkbox is enabled. SSL provides a more secure connection between the IaaS server and SQL database. However, you must first configure SSL on the SQL server to support this option. For more about configuring SSL on the SQL server, see Microsoft Technet article 189067.
13 Choose your database installation type from the Database Name panel.
   - Select Use existing empty database to create the schema in an existing database.
   - Enter a new database name or use the default name vra to create a new database. Database names must consist of no more than 128 ASCII characters.
14 Deselect Use default data and log directories to specify alternative locations or leave it selected to use the default directories (recommended).
15 Select an authentication method for installing the database from the **Authentication** list.

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

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

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

16 Click **Next**.

17 Complete the Prerequisite Check.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No errors</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Noncritical errors</td>
<td>Click <strong>Bypass</strong>.</td>
</tr>
<tr>
<td>Critical errors</td>
<td>Bypassing critical errors causes the installation to fail. If warnings appear, select the warning in the left pane and follow the instructions on the right. Address all critical errors and click <strong>Check Again</strong> to verify.</td>
</tr>
</tbody>
</table>

18 Click **Install**.

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

20 Click **Finish**.

The database is ready for use.

**Install an IaaS Website Component and Model Manager Data**

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

**Prerequisites**

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

1 Install the First IaaS Web Server Component
   You install the IaaS Web server component to provide access to infrastructure capabilities in vRealize Automation.

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

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

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

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

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

Procedure
1 If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.
   In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.

2 Right-click the setup_vrealize-automation-appliance-FQDN@5480.exe setup file and select Run as administrator.

3 Click Next.

4 Accept the license agreement and click Next.
On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.

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

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

b. Select Accept Certificate.

c. Click View Certificate.

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

6. Click Next.

7. Select Custom Install on the Installation Type page.

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

9. Accept the root install location or click Change and select an installation path.
   Even in a distributed deployment, you might sometimes install more than one IaaS component on the same Windows server.
   If you install more than one IaaS component, always install them to the same path.

10. Click Next.

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

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

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

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

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

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

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

This is a less secure option.

**Configure Model Manager Data**

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

**Prerequisites**

**Install the First IaaS Web Server Component.**

**Procedure**

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

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

   `vrealize-automation-appliance.mycompany.com`

   Do not enter an IP address.

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

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

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

   It might take several minutes to download the certificate.

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

6 Click **Accept Certificate**.

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

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

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

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

The default port is 443.

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

12 Complete the Prerequisite Check.

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

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

16 Click Next.

17 Click Install.

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

**What to do next**

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

**Install Additional IaaS Web Server Components**

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

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

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

Procedure

1. If using a load balancer, disable the other nodes under the load balancer, and verify that traffic is directed to the node that you want.
   
   In addition, disable load balancer health checks until all vRealize Automation components are installed and configured.

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

3. Click Next.

4. Accept the license agreement and click Next.

5. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   
   a. Type the user name, which is root, and the password.
   
   The password is the password that you specified when you deployed the vRealize Automation appliance.
   
   b. Select Accept Certificate.
   
   c. Click View Certificate.
   
   Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance.

6. Click Next.

7. Select Custom Install on the Installation Type page.

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

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

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

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

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

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

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

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

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

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

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

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

   This is a less secure option.

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

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

The default port is 443.

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

20 Click **Next**.
21 Complete the Prerequisite Check.

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

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

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

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

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

Keep this passphrase in a secure place for later use.

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

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

25 Click **Next**.

26 Click **Install**.

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

**What to do next**

**Install the Active Manager Service.**

**Install the Active Manager Service**

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

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

See **About Automatic Manager Service Failover.**
Prerequisites

- If you already installed other IaaS components, know the database passphrase that you created.
- (Optional) If you want to install the Manager Service in a Website other than the default Website, first create a Website in Internet Information Services.
- Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.
- Verify that the Website load balancer is configured and that the timeout value for the load balancer is set to a minimum of 180 seconds.
- Install an IaaS Website Component and Model Manager Data.

Procedure

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

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

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

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

The default port is 443.

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

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

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

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

16 Select the certificate for this component.

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

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

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

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

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

18 Click **Next**.

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

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

   The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.
21 Provide the passphrase used to generate the encryption key that protects the database.

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

Keep this passphrase in a secure place for later use.

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

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

23 Click Next.

24 Click Install.

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

26 Click Finish.

What to do next

- To ensure that the Manager Service you installed is the active instance, verify that the vCloud Automation Center Service is running and set it to “Automatic” startup type.

- You can install another instance of the Manager Service component as a passive backup that you can start manually if the active instance fails. See Install a Backup Manager Service Component.

- A system administrator can change the authentication method used to access the SQL database during run time (after the installation is complete). See Configuring Windows Service to Access the IaaS Database.

Install a Backup Manager Service Component

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

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

See About Automatic Manager Service Failover.

Prerequisites

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

- (Optional) If you want to install the Manager Service in a Web site other than the default Web site, first create a Web site in Internet Information Services.

- Use the vRealize Automation appliance management interface to replace the certificate to include the FQDN of the new node. See Replace Certificates in the vRealize Automation Appliance.
Verify that you have a certificate from a certificate authority imported into IIS and that the root certificate or certificate authority is trusted. All components under the load balancer must have the same certificate.

Verify that the Website load balancer is configured.

Install an IaaS Website Component and Model Manager Data.

**Procedure**

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

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

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

3. Click **Next**.

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

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

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

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

   b. Select **Accept Certificate**.

   c. Click **View Certificate**.

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

6. Click **Next**.

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

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

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

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

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

10. Click **Next**.

11. Select **Manager Service** on the **IaaS Server Custom Install** page.
In the **IaaS Server** text box, identify the IaaS Web server component.

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

The default port is 443.

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

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

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

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

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

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

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

19 Click **Next**.

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

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

The service account user must be one domain account that has privileges on each distributed IaaS server. Do not use local system accounts.
22 Provide the passphrase used to generate the encryption key that protects the database.

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

Keep this passphrase in a secure place for later use.

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

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

24 Click Next.

25 Click Install.

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

27 Click Finish.

What to do next

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

Installing Distributed Execution Managers

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

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

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

- DEM Orchestrators support active-active high availability. Typically, you install one DEM Orchestrator on each Manager Service machine.
- Install the Orchestrator on a machine with strong network connectivity to the Model Manager host.
- Install a second DEM Orchestrator on a different machine for failover.
- Typically, you install DEM Workers on the IaaS Manager Service server or on a separate server. The server must have network connectivity to the Model Manager host.
- You can install additional DEM instances for redundancy and scalability, including multiple instances on the same machine.
There are specific requirements for the DEM installation that depend on the endpoints you use. See IaaS Distributed Execution Manager Host.

Install the Distributed Execution Managers

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

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

Prerequisites

Download the vRealize Automation IaaS Installer.

Procedure

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

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

12 Click Next.

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

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

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

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

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

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

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

The default port is 443.

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

18 Click **Add**.

19 Click **Next**.

20 Click **Install**.

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

22 Click **Finish**.
What to do next

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

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

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

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

Prerequisites

- Know the non-default path where you installed the SCVMM console.
  
The following is the default path that you must replace in the configuration file.
  
  path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"

Procedure

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

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

3. Locate the <assemblyLoadConfiguration> section.
4. Update each path, using the following example as a guideline.

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

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

For more information, see DEM Workers with SCVMM.
Additional information about preparing the SCVMM environment and creating an SCVMM endpoint is available in Preparing Your SCVMM Environment and Create a Hyper-V (SCVMM) Endpoint.

Configuring Windows Service to Access the IaaS Database

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

Enable IaaS Database Access from the Service User

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

Prerequisites

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

Procedure

1. Navigate to the Database subdirectory within the directory where you extracted the installation zip archive.
2. Extract the DBInstall.zip archive to a local directory.
3. Log in to the database host as a user with the sysadmin role in the SQL Server instance.
4. Edit VMPSOpsUser.sql and replace all instances of $(Service User) with user (from Step 3) under which the Manager Service will run.
   Do not replace ServiceUser in the line ending with WHERE name = N'ServiceUser').
5. Open SQL Server Management Studio.
6. Select the database (vCAC by default) in Databases in the left-hand pane.
7. Click New Query.
   The SQL Query window opens in the right-hand pane.
8. Paste the modified contents of VMPS0psUser.sql into the query window.
9. Click Execute.

Database access is enabled from the Manager Service.

Configure the Windows Services Account to Use SQL Authentication

By default, the Windows service account accesses the database during run-time, even if you configured the database for SQL authentication. You can change run-time authentication from Windows to SQL.
One reason to change run-time authentication might be when, for example, the database is on an untrusted domain.

**Prerequisites**

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

**Procedure**

1. Using an account with administrator privileges, log in to the IaaS Windows server that hosts the Manager Service.

2. In Administrative Tools > Services, stop the VMware vCloud Automation Center service.

3. Open the following files in a text editor.

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

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

5. Replace `Integrated Security=True;` with `User Id=database-username;Password=database-password;`

6. Save and close the files.

7. Start the VMware vCloud Automation Center service.

8. Use the `iisreset` command to restart IIS.

**Verify IaaS Services**

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

**Procedure**

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

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

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

VMware vCloud Automation Center Service

3. Close the **Services** window.

## Installing vRealize Automation Agents

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

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

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

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

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

For information about using vSphere agents, see [vSphere Agent Requirements](#).

## Set the PowerShell Execution Policy to RemoteSigned

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

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

## Prerequisites

- Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.

- For more information about PowerShell Execution Policy, run `help about_signing` or `help Set-ExecutionPolicy` at the PowerShell command prompt.
Procedure

1. Using an administrator account, log in to the IaaS host machine where the agent is installed.
2. Select Start > All Programs > Windows PowerShell version > Windows PowerShell.
4. For Unrestricted, run Set-ExecutionPolicy Unrestricted.
5. Verify that the command did not produce any errors.
6. Type Exit at the PowerShell command prompt.

Choosing the Agent Installation Scenario

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

<table>
<thead>
<tr>
<th>Integration Scenario</th>
<th>Agent Requirements and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision cloud machines by integrating with a cloud environment such as Amazon Web Services or Red Hat Enterprise Linux OpenStack Platform.</td>
<td>You do not need to install an agent.</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a vSphere environment.</td>
<td>Installing and Configuring the Proxy Agent for vSphere</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a Microsoft Hyper-V Server environment.</td>
<td>Installing the Proxy Agent for Hyper-V or XenServer</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a XenServer environment.</td>
<td>Installing the Proxy Agent for Hyper-V or XenServer</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with a XenDesktop environment.</td>
<td>Installing the EPI Agent for Citrix</td>
</tr>
<tr>
<td>Run Visual Basic scripts as additional steps in the provisioning process before or after provisioning a machine, or when deprovisioning.</td>
<td>Installing the EPI Agent for Visual Basic Scripting</td>
</tr>
<tr>
<td>Collect data from the provisioned Windows machines, for example the Active Directory status of the owner of a machine.</td>
<td>Installing the WMI Agent for Remote WMI Requests</td>
</tr>
<tr>
<td>Provision virtual machines by integrating with any other supported virtual platform.</td>
<td>You do not need to install an agent.</td>
</tr>
</tbody>
</table>

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 1-38. Permissions Required for vSphere Agent to Manage vCenter Server Instance

<table>
<thead>
<tr>
<th>Attribute Value</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore</td>
<td>Allocate Space</td>
</tr>
<tr>
<td></td>
<td>Browse Datastore</td>
</tr>
<tr>
<td>Datastore Cluster</td>
<td>Configure a Datastore Cluster</td>
</tr>
<tr>
<td>Folder</td>
<td>Create Folder</td>
</tr>
<tr>
<td></td>
<td>Delete Folder</td>
</tr>
<tr>
<td>Global</td>
<td>Manage Custom Attributes</td>
</tr>
<tr>
<td></td>
<td>Set Custom Attribute</td>
</tr>
<tr>
<td>Network</td>
<td>Assign Network</td>
</tr>
<tr>
<td>Permissions</td>
<td>Modify Permission</td>
</tr>
<tr>
<td>Resource</td>
<td>Assign VM to Res Pool</td>
</tr>
<tr>
<td></td>
<td>Migrate Powered Off Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>Migrate Powered On Virtual Machine</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Inventory</td>
</tr>
<tr>
<td></td>
<td>Create from existing</td>
</tr>
<tr>
<td></td>
<td>Create New</td>
</tr>
<tr>
<td></td>
<td>Move</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>Interaction</td>
</tr>
<tr>
<td></td>
<td>Configure CD Media</td>
</tr>
<tr>
<td></td>
<td>Console Interaction</td>
</tr>
<tr>
<td></td>
<td>Device Connection</td>
</tr>
</tbody>
</table>
### Table 1-38. Permissions Required for vSphere Agent to Manage vCenter Server Instance (Continued)

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

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

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

Prerequisites

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

Procedure

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

The service must run on the same installation machine.

10 Click **Next**.

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers. Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.

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

16 Enter the name of the endpoint.

The endpoint name that you configure in vRealize Automation must match the endpoint name provided to the vSphere proxy agent during installation or the endpoint cannot function.
17 Click Add.
18 Click Next.
19 Click Install to begin the installation.

   After several minutes a success message appears.
20 Click Next.
21 Click Finish.
22 Verify that the installation is successful.

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

What to do next

Configure the vSphere Agent.

Configure the vSphere Agent

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

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

Prerequisites

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

Procedure

1 Open a Windows command prompt as an administrator.
2 Change to the agent installation folder, where agent-name is the folder containing the vSphere agent.
   cd %SystemDrive%\Program Files (x86)\VMware\vCAC\Agents\agent-name
3 (Optional) To view the current configuration settings, enter the following command.
   DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get

   The following is an example of the command output.

   managementEndpointName: VCendpoint
doDeletes: True

4 (Optional) To change the name of the endpoint that you configured at installation, use the following command.
   set managementEndpointName
For example: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

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

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

```
set doDeletes
```

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

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

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

**What to do next**

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

**Installing the Proxy Agent for Hyper-V or XenServer**

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

**Hyper-V and XenServer Requirements**

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

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

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

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

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

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

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

Prerequisites

- Install IaaS, including the Web server and Manager Service host.
- Download the vRealize Automation IaaS Installer.
- Verify that Hyper-V Hypervisor proxy agents have system administrator credentials.
- Verify that the credentials under which to run the agent service have administrative access to the installation host.
- Verify that all XenServer or Hyper-V instances on the hosts to be managed by the agent have administrator-level credentials.
- If you are using Xen pools, note that all nodes within the Xen pool must be identified by their fully qualified domain names.
  vRealize Automation cannot communicate with or manage any node that is not identified by its fully qualified domain name within the Xen pool.
- Configure Hyper-V for remote management to enable Hyper-V server communication with vRealize Automation Hyper-V proxy agents.
  See the Microsoft Windows Server documentation for information about how to configure Hyper-V for remote management.

Procedure

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

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

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

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

8 Click **Next**.

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

   The service must run on the same installation machine.

10 Click **Next**.

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

   - **Xen**
   - **Hyper-V**

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers. Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>

13 Communicate the **Agent name** to the IaaS administrator who configures endpoints.

   To enable access and data collection, the endpoint must be linked to the agent that was configured for it.

14 Configure a connection to the IaaS Manager Service host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
   | With a load balancer   | Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, `<load-balancer.fqdn>:443`.
   |                         | Do not enter IP addresses. |
   | Without a load balancer| Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, `<svc.fqdn>:443`.
   |                         | Do not enter IP addresses. |

   The default port is 443.
15 Configure a connection to the IaaS Web server.

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

The default port is 443.

16 Click Test to verify connectivity to each host.

17 Enter the credentials of a user with administrative-level permissions on the managed server instance.

18 Click Add.

19 Click Next.

20 (Optional) Add another agent.

   For example, you can add a Xen agent if you previously added the Hyper-V agent.

21 Click Install to begin the installation.

   After several minutes a success message appears.

22 Click Next.

23 Click Finish.

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.

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

4 Click **Start > Administrative Tools > Services** and restart the vRealize Automation Agent – `agentname` service.

**Example: Change Administrator-Level Credentials**

Enter the following command to change the administrator-level credentials for the virtualization platform specified during the agent installation.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

**What to do next**

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

**Installing the VDI Agent for XenDesktop**

vRealize Automation uses Virtual Desktop Integration (VDI) PowerShell agents to register the XenDesktop machines it provisions with external desktop management systems.

The VDI integration agent provides the owners of registered machines with a direct connection to the XenDesktop Web Interface. You can install a VDI agent as a dedicated agent to interact with a single Desktop Delivery Controller (DDC) or as a general agent that can interact with multiple DDCs.

**XenDesktop Requirements**

A system administrator installs a Virtual Desktop Infrastructure (VDI) agent to integrate XenDesktop servers into vRealize Automation.
You can install a general VDI agent to interact with multiple servers. If you are installing one dedicated agent per server for load balancing or authorization reasons, you must provide the name of the XenDesktop DDC server when installing the agent. A dedicated agent can handle only registration requests directed to the server specified in its configuration.

Consult the vRealize Automation Support Matrix on the VMware Web site for information about supported versions of XenDesktop for XenDesktop DDC servers.

**Installation Host and Credentials**

The credentials under which the agent runs must have administrative access to all XenDesktop DDC servers with which it interacts.

**XenDesktop Requirements**

The name given to the XenServer Host on your XenDesktop server must match the UUID of the Xen Pool in XenCenter. See Set the XenServer Host Name for more information.

Each XenDesktop DDC server with which you intend to register machines must be configured in the following way:

- The group/catalog type must be set to **Existing** for use with vRealize Automation.

- The name of a vCenter Server host on a DDC server must match the name of the vCenter Server instance as entered in the vRealize Automation vSphere endpoint, without the domain. The endpoint must be configured with a fully qualified domain name (FQDN), and not with an IP address. For example, if the address in the endpoint is `https://virtual-center27.domain/sdk`, the name of the host on the DDC server must be set to `virtual-center27`.

  If your vRealize Automation vSphere endpoint has been configured with an IP address, you must change it to use an FQDN. See **IaaS Configuration** for more information about setting up endpoints.

**XenDesktop Agent Host requirements**

Citrix XenDesktop SDK must be installed. The SDK for XenDesktop is included on the XenDesktop installation disc.

Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.

MS PowerShell Execution Policy is set to RemoteSigned or Unrestricted. See Set the PowerShell Execution Policy to RemoteSigned.

For more information about PowerShell Execution Policy, run `help about_signing` or `help Set-ExecutionPolicy` at the PowerShell command prompt.

**Set the XenServer Host Name**

In XenDesktop, the name given to the XenServer Host on your XenDesktop server must match the UUID of the Xen Pool in XenCenter. If no XenPool is configured, the name must match the UUID of the XenServer itself.
Procedure

1. In Citrix XenCenter, select your XenPool or standalone XenServer and click the **General** tab. Record the UUID.

2. When you add your XenServer Pool or standalone host to XenDesktop, type the UUID that was recorded in the previous step as the **Connection** name.

**Install the XenDesktop Agent**

Virtual desktop integration (VDI) PowerShell agents integrate with external virtual desktop system, such as XenDesktop and Citrix. Use a VDI PowerShell agent to manage the XenDesktop machine.

**Prerequisites**

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in [XenDesktop Requirements](#) have been met.
- Download the vRealize Automation IaaS Installer.

**Procedure**

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

2. Click **Next**.

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

4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   - Type the user name, which is `root`, and the password.
     - The password is the password that you specified when you deployed the vRealize Automation appliance.
   - Select **Accept Certificate**.
   - Click **View Certificate**.
     - Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance.
     - You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5. Click **Next**.

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

7. Select **Proxy Agents** in the Component Selection pane.

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

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

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

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

   The service must run on the same installation machine.

11 Click Next.

12 Select VdiPowerShell from the Agent type list.

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers. Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>

14 Configure a connection to the IaaS Manager Service host.

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

   The default port is 443.

15 Configure a connection to the IaaS Web server.

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

   The default port is 443.

16 Click Test to verify connectivity to each host.

17 Select the VDI version.

18 Enter the fully qualified domain name of the managed server in the VDI Server text box.
19 Click **Add**.

20 Click **Next**.

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

    After several minutes a success message appears.

22 Click **Next**.

23 Click **Finish**.

24 Verify that the installation is successful.

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

**What to do next**

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

**Installing the EPI Agent for Citrix**

External provisioning Integration (EPI) PowerShell agents integrate Citrix external machines into the provisioning process. The EPI agent provides on-demand streaming of the Citrix disk images from which the machines boot and run.

The dedicated EPI agent interacts with a single external provisioning server. You must install one EPI agent for each Citrix provisioning server instance.

**Citrix Provisioning Server Requirements**

A system administrator uses External Provisioning Infrastructure (EPI) agents to integrate Citrix provisioning servers and to enable the use of Visual Basic scripts in the provisioning process.

**Installation Location and Credentials**

Install the agent on the PVS host for Citrix Provisioning Services instances. Verify that the installation host meets **Citrix Agent Host Requirements** before you install the agent.

Although an EPI agent can generally interact with multiple servers, Citrix Provisioning Server requires a dedicated EPI agent. You must install one EPI agent for each Citrix Provisioning Server instance, providing the name of the server hosting it. The credentials under which the agent runs must have administrative access to the Citrix Provisioning Server instance.

Consult the **vRealize Automation Support Matrix** for information about supported versions of Citrix PVS.

**Citrix Agent Host Requirements**

PowerShell and Citrix Provisioning Services SDK must be installed on the installation host prior to agent installation. Consult the **vRealize Automation Support Matrix** on the VMware Web site for details.

Verify that Microsoft PowerShell is installed on the installation host before agent installation. The version required depends on the operating system of the installation host. See Microsoft Help and Support.
You must also ensure that the PowerShell Snap-In is installed. For more information, see the Citrix Provisioning Services PowerShell Programmer's Guide on the Citrix Web site.

MS PowerShell Execution Policy is set to RemoteSigned or Unrestricted. See Set the PowerShell Execution Policy to RemoteSigned.

For more information about PowerShell Execution Policy, run help about_signing or help Set-ExecutionPolicy at the PowerShell command prompt.

**Install the Citrix Agent**

External provisioning integration (EPI) PowerShell agents integrate external systems into the machine provisioning process. Use the EPI PowerShell agent to integrate with Citrix provisioning server to enable provisioning of machines by on-demand disk streaming.

**Prerequisites**

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in Citrix Provisioning Server Requirements have been met.
- Download the vRealize Automation IaaS Installer.

**Procedure**

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

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

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

8  Click **Next**.

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

The service must run on the same installation machine.

10 Click **Next**.

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers.</td>
</tr>
<tr>
<td></td>
<td>Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

14 Configure a connection to the IaaS Web server.

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

The default port is 443.
15 Click **Test** to verify connectivity to each host.

16 Select the EPI type.

17 Enter the fully qualified domain name of the managed server in the **EPI Server** text box.

18 Click **Add**.

19 Click **Next**.

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

   After several minutes a success message appears.

21 Click **Next**.

22 Click **Finish**.

23 Verify that the installation is successful.

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

**What to do next**

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

**Installing the EPI Agent for Visual Basic Scripting**

A system administrator can specify Visual Basic scripts as additional steps in the provisioning process before or after provisioning a machine, or when deprovisioning a machine. You must install an External Provisioning Integration (EPI) PowerShell before you can run Visual Basic scripts.

Visual Basic scripts are specified in the blueprint from which machines are provisioned. Such scripts have access to all of the custom properties associated with the machine and can update their values. The next step in the workflow then has access to these new values.

For example, you could use a script to generate certificates or security tokens before provisioning and use them in machine provisioning.

To enable scripts in provisioning, you must install a specific type of EPI agent and place the scripts you want to use on the system on which the agent is installed.

When executing a script, the EPI agent passes all machine custom properties as arguments to the script. To return updated property values, you must place these properties in a dictionary and call a vRealize Automation function. A sample script is included in the scripts subdirectory of the EPI agent installation directory. This script contains a header to load all arguments into a dictionary, a body in which you can include your function(s), and a footer to return updated custom properties values.

**Note** You can install multiple EPI/VBScripts agents on multiple servers and provision using a specific agent and the Visual Basic scripts on that agent’s host. If you need to do this, contact VMware customer support.
**Visual Basic Scripting Requirements**

A system administrator installs External Provisioning Infrastructure (EPI) agents to enable the use of Visual Basic scripts in the provisioning process.

The following table describes the requirements that apply to installing an EPI agent to enable the use of Visual Basic scripts in the provisioning process.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>Credentials under which the agent will run must have administrative access to the installation host.</td>
</tr>
<tr>
<td>Microsoft PowerShell</td>
<td>Microsoft PowerShell must be installed on the installation host prior to agent installation: The version required depends on the operating system of the installation host and might have been installed with that operating system. Visit <a href="http://support.microsoft.com">http://support.microsoft.com</a> for more information.</td>
</tr>
<tr>
<td>MS PowerShell Execution Policy</td>
<td>MS PowerShell Execution Policy must be set to <strong>RemoteSigned</strong> or <strong>Unrestricted</strong>. For information on PowerShell Execution Policy issue one of the following commands at Power-Shell command prompt:</td>
</tr>
</tbody>
</table>

**Install the Agent for Visual Basic Scripting**

External provisioning integration (EPI) PowerShell agents allow integrate external systems into the machine provisioning process. Use an EPI agent to run Visual Basic Scripts as extra steps during the provisioning process.

**Prerequisites**

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in **Visual Basic Scripting Requirements** have been met.
- Download the vRealize Automation IaaS Installer.

**Procedure**

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

a Type the user name, which is **root**, and the password.
   The password is the password that you specified when you deployed the vRealize Automation appliance.

b Select **Accept Certificate**.

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

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

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

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

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

Click **Next**.

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

Click **Next**.

Select **EPIPowerShell** from the Agent type list.

Enter an identifier for this agent in the **Agent name** text box.
Maintain a record of the agent name, credentials, endpoint name, and platform instance for each agent. You need this information to configure endpoints and to add hosts in the future.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers.</td>
</tr>
<tr>
<td></td>
<td>Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>
Configure a connection to the IaaS Manager Service host.

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

The default port is 443.

Configure a connection to the IaaS Web server.

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

The default port is 443.

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

Select the EPI type.

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

Click **Add**.

Click **Next**.

Click **Install** to begin the installation.

After several minutes a success message appears.

Click **Next**.

Click **Finish**.

Verify that the installation is successful.

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

**Installing the WMI Agent for Remote WMI Requests**

A system administrator enables the Windows Management Instrumentation (WMI) protocol and installs the WMI agent on all managed Windows machines to enable management of data and operations. The agent is required to collect data from Windows machines, such as the Active Directory status of the owner of a machine.
Enable Remote WMI Requests on Windows Machines

To use WMI agents, remote WMI requests must be enabled on the managed Windows servers.

Procedure

1. In each domain that contains provisioned and managed Windows virtual machines, create an Active Directory group and add to it the service credentials of the WMI agents that execute remote WMI requests on the provisioned machines.

2. Enable remote WMI requests for the Active Directory groups containing the agent credentials on each Windows machine provisioned.

Install the WMI Agent

The Windows Management Instrumentation (WMI) agent enables data collection from Windows managed machines.

Prerequisites

- Install IaaS, including the Web server and Manager Service host.
- Verify that the requirements in Enable Remote WMI Requests on Windows Machines have been met.
- Download the vRealize Automation IaaS Installer.

Procedure

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

2. Click Next.

3. Accept the license agreement and click Next.

4. On the Log in page, supply administrator credentials for the vRealize Automation appliance and verify the SSL Certificate.
   a. Type the user name, which is root, and the password.
      The password is the password that you specified when you deployed the vRealize Automation appliance.
   b. Select Accept Certificate.
   c. Click View Certificate.
      Compare the certificate thumbprint with the thumbprint set for the vRealize Automation appliance. You can view the vRealize Automation appliance certificate in the client browser when the management console is accessed on port 5480.

5. Select Custom Install on the Installation Type page.

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

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

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

8 Click Next.

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

The service must run on the same installation machine.

10 Click Next.

11 Select WMI from the Agent type list.

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant agent</td>
<td>Install redundant agents on different servers. Name and configure redundant agents identically.</td>
</tr>
<tr>
<td>Standalone agent</td>
<td>Assign a unique name to the agent.</td>
</tr>
</tbody>
</table>

13 Configure a connection to the IaaS Manager Service host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>With a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Manager Service component, \textit{mgr-svc-load-balancer.mycompany.com:443}. Do not enter IP addresses.</td>
</tr>
<tr>
<td>Without a load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Manager Service component, \textit{mgr-svc.mycompany.com:443}. Do not enter IP addresses.</td>
</tr>
</tbody>
</table>

The default port is 443.

14 Configure a connection to the IaaS Web server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>With a load balancer</td>
<td>Enter the fully qualified domain name and port number of the load balancer for the Web server component, \textit{web-load-balancer.mycompany.com:443}. Do not enter IP addresses.</td>
</tr>
<tr>
<td>Without a load balancer</td>
<td>Enter the fully qualified domain name and port number of the machine where you installed the Web server component, \textit{web.mycompany.com:443}. Do not enter IP addresses.</td>
</tr>
</tbody>
</table>

The default port is 443.
15 Click **Test** to verify connectivity to each host.

16 Click **Add**.

17 Click **Next**.

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

   After several minutes a success message appears.

19 Click **Next**.

20 Click **Finish**.

21 Verify that the installation is successful.

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

**Silent vRealize Automation Installation**

vRealize Automation includes options for scripted, silent installation from the command line, and API-based silent installation. Both approaches require that you prepare, in advance, the values that you would normally enter by hand during a conventional installation.

**About Silent vRealize Automation Installation**

vRealize Automation silent installation uses an executable that references a text-based answer file.

In the answer file, you preconfigure system FQDNs, account credentials, and other settings that you typically add throughout a conventional wizard-based or manual installation. Silent installation is useful for the following kinds of deployments.

- Deploying multiple, nearly identical environments
- Repeatedly redeploying the same environment
- Performing unattended installations
- Performing scripted installations

**Perform a Silent vRealize Automation Installation**

You can perform an unattended, silent vRealize Automation installation from the console of a newly deployed vRealize Automation appliance.

**Prerequisites**

- Create an unconfigured appliance. See [Deploy the vRealize Automation Appliance](#).
- Create or identify your IaaS Windows servers, and configure their prerequisites.
- Install the Management Agent on your IaaS Windows servers.

   You may install the Management Agent using the traditional `.msi` file download or the silent process described in [Perform a Silent vRealize Automation Management Agent Installation](#).
Procedure

1. Log in to the vRealize Automation appliance console as root.
2. Navigate to the following directory.
   /usr/lib/vcac/tools/install
3. Open the ha.properties answer file in a text editor.
4. Add entries specific to your deployment in ha.properties, and save and close the file.
   Alternatively, you can save time by copying and modifying an ha.properties file from another deployment instead of editing the entire default file.
5. From the same directory, start the installation by running the following command.
   vra-ha-config.sh
   Installation might take up to an hour or more to complete, depending on the environment and size of the deployment.
6. (Optional) After installation finishes, review the log file.
   /var/log/vcac/vra-ha-config.log
   The silent installer does not save proprietary data to the log, such as passwords, licenses, or certificates.

Perform a Silent vRealize Automation Management Agent Installation

You can perform a command line based vRealize Automation Management Agent installation on any IaaS Windows server.

Silent Management Agent installation consists of a Windows PowerShell script in which you customize a few settings. After adding your deployment-specific settings, you can silently install the Management Agent on all of your IaaS Windows servers by running copies of the same script on each one.

Prerequisites

- Create an unconfigured appliance. See Deploy the vRealize Automation Appliance.
- Create or identify your IaaS Windows servers, and configure their prerequisites.

Procedure

1. Log in to the IaaS Windows server using an account that has administrator rights.
2. Open a Web browser to the vRealize Automation appliance installer URL.
   https://vrealize-automation-appliance-FQDN:5480/installer
3. Right-click the link to the InstallManagementAgent.ps1 PowerShell script file, and save it to the desktop or a folder on the IaaS Windows server.
4. Open InstallManagementAgent.ps1 in a text editor.
Near the top of the script file, add your deployment-specific settings.

- The vRealize Automation appliance URL
  https://vrealize-automation-appliance-FQDN:5480
- vRealize Automation appliance root user account credentials
- vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers
- The folder where you want to install the Management Agent, Program Files (x86) by default
- (Optional) The thumbprint of the PEM format certificate that you are using for authentication

Save and close InstallManagementAgent.ps1.

To silently install the Management Agent, double-click InstallManagementAgent.ps1.

(Optional) Verify that installation has finished by locating VMware vCloud Automation Center Management Agent in the Windows Control Panel list of Programs and Features, and in the list of Windows services that are running.

Silent vRealize Automation Installation Answer File

Silent vRealize Automation installations require that you prepare a text-based answer file in advance. All newly deployed vRealize Automation appliances contain a default answer file.

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

To perform a silent installation, you must use a text editor to customize the settings in ha.properties to the deployment that you want to install. The following examples are a few of the settings and information that you must add.

- Your vRealize Automation or suite license key
- vRealize Automation appliance node FQDNs
- vRealize Automation appliance root user account credentials
- IaaS Windows server FQDNs that will act as Web nodes, Manager Service nodes, and so on
- vRealize Automation service user credentials, a domain account with administrator privileges on the IaaS Windows servers
- Load balancer FQDNs
- SQL Server database parameters
- Proxy agent parameters to connect to virtualization resources
- Whether the silent installer should attempt to correct missing IaaS Windows server prerequisites

The silent installer can correct many missing Windows prerequisites. However, some configuration problems, such as not enough CPU, cannot be changed by the silent installer.
To save time, you can reuse and modify an ha.properties file that was configured for another deployment, one where the settings were similar. Also, when you install vRealize Automation non-silently through the Installation Wizard, the wizard creates and saves your settings in the ha.properties file. The file might be useful to reuse and modify for silently installing a similar deployment.

The wizard does not save proprietary settings to the ha.properties file, such as passwords, licenses, or certificates.

**The vRealize Automation Installation Command Line**

vRealize Automation includes a console-based, command line interface for performing installation adjustments that might be required after initial installation.

The command line interface (CLI) can run installation and configuration tasks that are no longer available through the browser-based interface after initial installation. CLI features include rechecking prerequisites, installing IaaS components, installing certificates, or setting the vRealize Automation host name to which users point their Web browser.

The CLI is also useful for advanced users who want to script certain operations. Some CLI functions are used by silent installation, so familiarity with both features reinforces your knowledge of vRealize Automation installation scripting.

### vRealize Automation Installation Command-Line Basics

The vRealize Automation installation command-line interface includes top-level, basic operations.

The basic operations display vRealize Automation node IDs, run commands, report command status, or display the help information. To show these operations and their options at the console display, enter the following command without any options or qualifiers.

```
vra-command
```

**Display Node IDs**

You need vRealize Automation node IDs so that you can run commands against the correct target systems. To display node IDs, enter the following command.

```
vra-command list-nodes
```

Make note of node IDs before running commands against specific machines.

**Run Commands**

Most command-line functions involve running a command against a node in the vRealize Automation cluster. To run a command, use the following syntax.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

As shown in the preceding syntax, many commands require parameters, and parameter values, selected by the user.
Display Command Status

Some commands take a few moments or even longer to finish. To monitor the progress of a command that was entered, enter the following command.

vra-command status

The status command is especially valuable for monitoring a silent install, which can take a long time for large deployment sizes.

Display Help

To display help for all available commands, enter the following command.

vra-command help

To display help for a single command, enter the following command.

vra-command help command-name

vRealize Automation Installation Command Names

Commands give you console access to many vRealize Automation installation and configuration tasks that you might want to perform after initial installation.

Examples of available commands include the following functions.

- Adding another vRealize Automation appliance to an existing installation
- Setting the host name that users point a Web browser to when they access vRealize Automation
- Creating the IaaS SQL Server database
- Running the prerequisite checker against an IaaS Windows server
- Importing certificates

For a complete list of available vRealize Automation commands, log in to the vRealize Automation appliance console, and enter the following command.

vra-command help

The long list of command names and parameters is not reproduced in separate documentation. To use the list effectively, identify a command of interest, and narrow your focus by entering the following command.

vra-command help command-name

The vRealize Automation Installation API

The vRealize Automation REST API for installation gives you the ability to create purely software-controlled installations for vRealize Automation.
The installation API requires a JSON formatted version of the same entries that the CLI based installation obtains from the ha.properties answer file. The following guidelines familiarize you with how the API works. From there, you should be able to design programmatic calls to the API to install vRealize Automation.

- To access the API documentation, point a Web browser to the following vRealize Automation appliance page.

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

  You need an unconfigured vRealize Automation appliance. See Deploy the vRealize Automation Appliance.

- To experiment with the API based installation, locate and expand the following PUT command.

  PUT /vra-install

- Copy the unpopulated JSON from the install_json box to a text editor. Fill in the answer values the same way that you would for ha.properties. When your JSON formatted answers are ready, copy the code back to install_json and overwrite the unpopulated JSON.

  Alternatively, you can edit the following template JSON and copy the result to install_json.

  /usr/lib/vcac/tools/install/installationProperties.json

  You can also convert a completed ha.properties to JSON or vice versa.

- In the action box, select validate and click Try It Out.

  The validate action runs the vRealize Automation prerequisite checker and fixer.

- The validate response includes an alphanumeric command ID that you can insert into the following GET command.

  GET /commands/command-id/aggregated-status

  The response to the GET includes the progress of the validation operation.

- When validation succeeds, you can run the actual installation by repeating the process. In the action box, just select install instead of validate.

  Installation can take a long time depending on the deployment size. Again, locate the command ID, and use the aggregated status GET command to obtain installation progress. The GET response might resemble the following example.

  "progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18, "queued": 3, "processing": 1}, "failed-commands": 0

- If something goes wrong with the installation, you can trigger log collection for all nodes using the following command.

  PUT /commands/log-bundle

  Similar to installation, the returned alphanumeric command ID lets you monitor log collection status.
Convert Between vRealize Automation Silent Properties and JSON

For silent vRealize Automation CLI or API based installations, you can convert a completed properties answer file to JSON or vice versa. The silent CLI installation requires the properties file, while the API requires JSON format.

Prerequisites

A completed properties answer file or completed JSON file

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

or

/usr/lib/vcac/tools/install/installationProperties.json

Procedure

1. Log in to a vRealize Automation appliance console session as root.
2. Run the appropriate converter script.
   - Convert JSON to Properties
     /usr/lib/vcac/tools/install/convert-properties --from-json installationProperties.json
     The script creates a new properties file with the timestamp in the name, for example:
     ha.2016-10-17_13.02.15.properties
   - Convert Properties to JSON
     /usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
     The script creates a new installationProperties.json file with the timestamp in the name, for example:
     installationProperties.2016-10-17_13.36.13.json

You can also display help for the script.

/usr/lib/vcac/tools/install/convert-properties --help

vRealize Automation Post-Installation Tasks

After you install vRealize Automation, there are post-installation tasks that might need your attention.

Configure Federal Information Processing Standard Compliant Encryption

You can enable or disable Federal Information Processing Standard (FIPS) 140–2 compliant cryptography for inbound and outbound vRealize Automation appliance network traffic.

Changing the FIPS setting requires a vRealize Automation restart. FIPS is disabled by default.
Procedure

1 Log in as root to the vRealize Automation appliance management interface.
   https://vrealize-automation-appliance-FQDN:5480

2 Click vRA Settings > Host Settings.

3 Near the upper right, click the button to enable or disable FIPS.

   When enabled, inbound and outbound vRealize Automation appliance network traffic on port 443 uses FIPS 140–2 compliant encryption. Regardless of the FIPS setting, vRealize Automation uses AES–256 compliant algorithms to protect secured data stored on the vRealize Automation appliance.

   **Note**  This vRealize Automation release only partially enables FIPS compliance, because some internal components do not yet use certified cryptographic modules. In cases where certified modules have not yet been implemented, the AES–256 compliant algorithms are used.

4 Click Yes to restart vRealize Automation.

You can also configure FIPS from a vRealize Automation appliance console session as root, using the following commands.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Enable Automatic Manager Service Failover

Automatic Manager Service failover is disabled by default if you install or upgrade the Manager Service with the standard vRealize Automation Windows installer.

To enable automatic Manager Service failover after running the standard Windows installer, take the following steps.

Procedure

1 Log in as root to a console session on the vRealize Automation appliance.

2 Navigate to the following directory.
   `/usr/lib/vcac/tools/vami/commands`

3 Enter the following command.
   ```
   python ./manager-service-automatic-failover ENABLE
   ```

   If you need to disable automatic failover throughout an IaaS deployment, enter the following command instead.

   ```
   python ./manager-service-automatic-failover DISABLE
   ```
About Automatic Manager Service Failover

You can configure the vRealize Automation IaaS Manager Service to fail over to a backup when the primary Manager Service stops.

Starting in vRealize Automation 7.3, you no longer have to manually start or stop the Manager Service on each Windows server, to control which serves as primary or backup. Automatic Manager Service failover is enabled by default in the following cases.

- When you install vRealize Automation silently or with the Installation Wizard.
- When you upgrade IaaS through the administration interface or with the automatic upgrade script.

Failover is not enabled when you use the standard Windows-based installer to add a Manager Service host or upgrade IaaS. To enable it, see Enable Automatic Manager Service Failover.

When automatic failover is enabled, the Manager Service automatically starts on all Manager Service hosts, including backups. The automatic failover feature allows hosts to transparently monitor each other and fail over when necessary. The feature requires that the Windows service is running on all hosts.

**Note**  You are not required to use automatic failover. You may disable it and continue to manually start and stop the Windows service to control which host serves as primary or backup. If you take the manual failover approach, you must only start the service on one host at a time. With automatic failover disabled, simultaneously running the service on multiple IaaS servers makes vRealize Automation unusable.

- Do not attempt to selectively enable or disable automatic failover. Automatic failover must always be synchronized as on or off, across every Manager Service host in an IaaS deployment.

If automatic failover does not appear to be working, see Automatic Manager Service Failover Does Not Activate for troubleshooting tips.

Automatic vRealize Automation PostgreSQL Database Failover

In a high availability vRealize Automation deployment, some configurations allow the embedded vRealize Automation PostgreSQL database to fail over automatically.

Automatic failover is silently enabled under the following conditions.

- The high availability deployment includes three vRealize Automation appliances.
  
  Automatic failover is not supported with only two appliances.

- Database replication is set to Synchronous Mode in vRA Settings > Database in the vRealize Automation administration interface.

Usually, you should avoid performing a manual failover while automatic failover is enabled. However, for some node problems, automatic failover might not occur even though it is enabled. When that happens, check to see if you need to perform a manual failover.

1. After the primary PostgreSQL database node fails, wait up to 5 minutes for the rest of the cluster to stabilize.
2 On a surviving vRealize Automation appliance node, open a browser to the following URL.
   https://vrealize-automation-appliance-FQDN:5434/api/status
3 Search for manualFailoverNeeded.
4 If manualFailoverNeeded is true, perform a manual failover.

For more information, see Perform Manual vRealize Automation Appliance Database Failover.

Replacing Self-Signed Certificates with Certificates Provided by an Authority

If you installed vRealize Automation with self-signed certificates, you might want to replace them with certificates provided by a certificate authority before deploying to production.

For more information about updating certificates, see Updating vRealize Automation Certificates.

Changing Host Names and IP Addresses

In general, you should expect to keep the host names, FQDNs, and IP addresses that you planned for vRealize Automation systems. Some post-installation changes are possible but can be complicated.

- If you change the host name of the Windows machine that hosts the IaaS SQL Server database, see Configure the SQL Database for a New Host Name.
- When restoring IaaS components, renaming a host can affect the IaaS Web host, Manager Service host, or their respective load balancers. Restore these hosts or load balancers according to the vRealize Suite backup and restore instructions.

To change a vRealize Automation appliance host name or IP address, see the following sections.

Change the vRealize Automation Appliance Host Name

When maintaining an environment or network, you might need to assign a different host name to a vRealize Automation appliance.

**Important** Renaming takes vRealize Automation offline for several minutes.

The same steps apply for standalone, master, and replica vRealize Automation appliances.

**Procedure**

1 In DNS, create an additional record with the new node host name.
   Do not remove the existing DNS record with the old host name yet.
2 Wait for DNS replication and zone distribution to occur.
3 Log in as root to the vRealize Automation appliance command line.
4 Run the following command.
   `vcac-config hostname-change --host new-hostname --certificate certificate-file-name`
A certificate file is optional unless the old appliance host name was used in a certificate. If so, supply an updated certificate that has the new host name.

When you specify a certificate file, the renaming command also imports the certificate and returns the certificate ID.

A certificate file must be in the same format as the text output of the /config/ssl/generate-certificate API command and contain the new DNS name in its SAN field.

5 Wait up to 15 minutes or more for the renaming process to finish. The command actions take a few minutes, followed by several additional minutes for service re-registration.

6 If the old appliance host name was used with a load balancer in an HA environment, check and reconfigure the load balancer with the new name.

7 In DNS, remove the existing DNS record with the old host name.

If you have problems changing a host name, try the separate procedures from the vRealize Automation 7.3 documentation instead.

Change the vRealize Automation Appliance IP Address

When maintaining an environment or network, you might need to assign a different IP address to an existing vRealize Automation appliance.

Prerequisites

- As a precaution, take snapshots of vRealize Automation appliances and IaaS servers.
- From a console session as root on the vRealize Automation appliances, inspect entries in the /etc/hosts file.
  Look for address assignments that might conflict with the new IP address plan, and make changes as needed.
  
  On all IaaS servers, repeat the process for the Windows\system32\drivers\etc\hosts file.
- Shut down all vRealize Automation appliances.
- Stop all vRealize Automation services on IaaS servers.

Procedure

1 In vSphere, locate the vRealize Automation appliance that you want to change, and select Actions > Edit Settings.

2 Click vApp Options.

3 Expand IP allocation, and enable the OVF environment option.
4 Expand **OVF Settings**, and enable the **ISO image** option.

**Figure 1-16. OVF Environment and ISO Image Options**

5 Click **OK**.

6 Start the vRealize Automation appliance that you are changing.

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

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

8 Click the **Network** tab.

9 Below the tabs, click **Address**.

10 Update the IP address.

11 At the upper right, click **Save Settings**.

12 Shut down the vRealize Automation appliance that you are changing.
In DNS, update entries for the new IP addresses.

Only update existing A-type records. Do not change FQDNs.

If using a load balancer, also update load balancer IP settings for back-end nodes, service pools, and virtual servers as needed.

Wait for DNS replication and zone distribution to occur.

Start all vRealize Automation appliances.

Start vRealize Automation services on IaaS servers.

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

Verify vRealize Automation appliance status in the following areas.

- Database connection status under vRA Settings > Database
- RabbitMQ status under vRA Settings > Messaging
- Xenon status under vRA Settings > Xenon
- All services as REGISTERED under Services

Adjusting the SQL Database for a Changed Host Name

You must revise configuration settings if you move the vRealize Automation IaaS SQL database to a different host name.

On the same host name, you can restore the SQL database from a backup with no further steps required. If you restore to a different host name, you need to edit configuration files to make additional changes.

See VMware Knowledge Base article 2074607 for the changes required when moving the SQL database to a different host name.

Change an IaaS Server IP Address

When maintaining an environment or network, you might need to assign a different IP address to an existing vRealize Automation IaaS Windows server.

Prerequisites

- If the vRealize Automation appliance IP address needs to change, do that first. See Change the vRealize Automation Appliance IP Address.
- As a precaution, take snapshots of vRealize Automation appliances and IaaS servers.
- From a console session as root on the vRealize Automation appliance, inspect entries in the /etc/hosts file.

Look for address assignments that might conflict with the new IP address plan, and make changes as needed.

On all IaaS servers, repeat the process for the Windows\system32\drivers\etc\hosts file.
Shut down the vRealize Automation appliance.

Stop all vRealize Automation services on IaaS servers.

**Procedure**

1. Log in to the IaaS server with an account that has administrator rights.
2. In Windows, change the IP address.
   
   Look for the IP address in the Windows network adapter settings, under Internet Protocol properties.
3. Refresh your local DNS with the changes.
   
   Refreshing DNS ensures that the IaaS Windows servers can find each other and that you can reconnect to a Windows server if you are disconnected.
4. On the Manager Service host, inspect the following file in a text editor.
   
   \( \text{install-fold}e r\backslash vC A C \backslash S e r v e r \backslash M a n a g e r S e r v i c e . e x e . c o n f i g \)
   
   The default install folder is \( C: \backslash P r o g r a m \ F i l e s \ ( x 8 6 ) \backslash V M w a r e . \)
   
   Verify IP addresses or FQDNs of vRealize Automation appliances and IaaS Windows servers.
5. On all IaaS Windows servers, inspect the following file in a text editor.
   
   \( \text{install-fold}e r\backslash vC A C \backslash M a n a g e m e n t \ A g e n t \backslash V M w a r e . I a a s . M a n a g e m e n t . A g e n t . e x e . C o n f i g \)
   
   Verify the IP address or FQDN of the vRealize Automation appliance.
6. Log in to the SQL Server host.
7. Verify that the repository address is correctly configured to use FQDN in the ConnectionString column.
   
   For example, open SQL Management Studio and run the following query.
   
   "SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].[Models]"
8. Start the vRealize Automation appliance.
9. Start vRealize Automation services on IaaS servers.
10. Inspect log files to verify that Agent, DEM Worker, Manager Service, and Web host services started successfully.
11. Log in to vRealize Automation as a user with the Infrastructure Administrator role.
12. Navigate to **Infrastructure > Monitoring > Distributed Execution Status** and verify that all services are running.
13. Test for correct operation by checking appliance services, testing provisioning, or using the vRealize Production Test tool.
Change an IaaS Server Host Name

When maintaining an environment or network, you might need to assign a different host name to an existing vRealize Automation IaaS Windows server.

Procedure

1. Take a snapshot of the IaaS server.
2. On the IaaS server, use IIS Manager to stop the vRealize Automation application pools: Repository, VMware vRealize Automation, and Wapi.
3. On the IaaS server, use Administrative Tools > Services to stop all vRealize Automation services, agents, and DEMs.
4. In DNS, create an additional record with the new host name.
   Do not remove the existing DNS record with the old host name yet.
5. Wait for DNS replication and zone distribution to occur.
6. On the IaaS server, change the host name, but do not restart when prompted.
   Look for the host name in the Windows system properties, under the computer name, domain, and workgroup settings.
   When prompted to restart, click the option to restart later.
7. If you used the old host name to generate certificates, update certificates.
   For more information, see Updating vRealize Automation Certificates.
8. Use a text editor to locate and update the host name inside configuration files.
   Make the updates based on which IaaS server host name you changed. In a distributed HA deployment, you might need to access more than one server. There are no updates if you change the host name of a DEM Orchestrator or DEM Worker.

Note: Only update the old Windows server host name. If you find a load balancer name instead, keep the load balancer name.

Table 1-40. Files to Update When Changing a Web Node Host Name

<table>
<thead>
<tr>
<th>IaaS Server</th>
<th>Path</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web nodes</td>
<td>install-folder\Server\Website</td>
<td>Web.config</td>
</tr>
<tr>
<td></td>
<td>install-folder\Server\Website\Cafe</td>
<td>Vcac-Config.exe.config</td>
</tr>
<tr>
<td></td>
<td>install-folder\Web API</td>
<td>Web.config</td>
</tr>
<tr>
<td></td>
<td>install-folder\Web API\ConfigTool</td>
<td>Vcac-Config.exe.config</td>
</tr>
<tr>
<td>Node with the Model Manager component</td>
<td>install-folder\Server\Model Manager Data</td>
<td>Repoutil.exe.config</td>
</tr>
<tr>
<td>installed</td>
<td>install-folder\Server\Model Manager Data\Cafe</td>
<td>Vcac-Config.exe.config</td>
</tr>
<tr>
<td>Manager Service nodes</td>
<td>install-folder\Server</td>
<td>ManagerService.exe.config</td>
</tr>
</tbody>
</table>
Table 1-40. Files to Update When Changing a Web Node Host Name (Continued)

<table>
<thead>
<tr>
<th>IaaS Server</th>
<th>Path</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM Orchestrator nodes</td>
<td>install-folder\Distributed Execution Manager\dem</td>
<td>DynamicOps.DEM.exe.config</td>
</tr>
<tr>
<td>DEM Worker nodes</td>
<td>install-folder\Distributed Execution Manager\DEM-name</td>
<td>DynamicOps.DEM.exe.config</td>
</tr>
<tr>
<td>Agent nodes</td>
<td>install-folder\Agents\agent-name</td>
<td>RepoUtil.exe.config</td>
</tr>
<tr>
<td></td>
<td>install-folder\Agents\agent-name</td>
<td>VRMAgent.exe.config</td>
</tr>
</tbody>
</table>

Table 1-41. Files to Update When Changing a Manager Service Node Host Name

<table>
<thead>
<tr>
<th>IaaS Server</th>
<th>Path</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM Orchestrator nodes</td>
<td>install-folder\Distributed Execution Manager\DEM-name</td>
<td>DynamicOps.DEM.exe.config</td>
</tr>
<tr>
<td>DEM Worker nodes</td>
<td>install-folder\Distributed Execution Manager\DEM-name</td>
<td>DynamicOps.DEM.exe.config</td>
</tr>
<tr>
<td>Agent nodes</td>
<td>install-folder\Agents\agent-name</td>
<td>VRMAgent.exe.config</td>
</tr>
</tbody>
</table>

Table 1-42. Files to Update When Changing an Agent Node Host Name

<table>
<thead>
<tr>
<th>IaaS Server</th>
<th>Path</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent node</td>
<td>install-folder\Agents\agent-name</td>
<td>VRMAgent.exe.config</td>
</tr>
</tbody>
</table>

9 Restart the IaaS server where you changed the host name.

10 Start the vRealize Automation application pools that you stopped earlier.

11 Start the vRealize Automation services, agents, and DEMs that you stopped earlier.

12 If the old IaaS server host name was used with a load balancer in an HA environment, check and reconfigure the load balancer with the new name.

13 In DNS, remove the existing DNS record with the old host name.

14 Wait for DNS replication and zone distribution to occur.

15 If you changed the host name of a Manager Service host, take the following additional steps.
   a Update software agents on existing virtual machines.
   b Recreate any ISOs or templates that contain a guest agent.

What to do next

Validate that vRealize Automation is ready for use. See the vRealize Suite Backup and Restore documentation.

Set the vRealize Automation Login URL to a Custom Name

If you want vRealize Automation users to log in to a URL name other than the vRealize Automation appliance or load balancer name, take customization steps before and after installation.
Procedure

1. Before installing, prepare a certificate that includes the CNAME that you want, as well as vRealize Automation appliance and load balancer names.

2. Install vRealize Automation, entering the appliance or load balancer name as usual. During installation, import the customized certificate.

3. After installing, in DNS, create a CNAME alias of Common Name, and point it to the appliance or load balancer VIP address.

4. Log in to the vRealize Automation appliance administrator interface as root.

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

5. Under vRA Settings > Host Settings, change the Host Name to the CNAME that you chose.

Licensing vRealize Code Stream

You can enable vRealize Code Stream by entering a vRealize Code Stream license in vRealize Automation.

You can enter the vRealize Code Stream license in either of these locations:

- On the Licensing page of the vRealize Automation installation wizard. For more information, see vRealize Code Stream Installation.
- On the Licensing tab in the vRealize Automation appliance management interface. For more information, see Apply a vRealize Code Stream License to an Appliance.

Installing the vRealize Log Insight Agent on IaaS Servers

The Windows servers in a vRealize Automation IaaS configuration do not include the vRealize Log Insight agent by default.

vRealize Log Insight provides log aggregation and indexing, and can collect, import, and analyze logs to expose system problems. If you want to capture and analyze logs from IaaS servers by using vRealize Log Insight, you must separately install the vRealize Log Insight agent for Windows.

For more information, see the VMware vRealize Log Insight documentation.

vRealize Automation appliances include the vRealize Log Insight agent by default.

Change the VMware Remote Console Proxy Port

If your site blocks or otherwise reserves port 8444, you can change the default proxy port used by VMware Remote Console.

Procedure

1. Access the vRealize Automation appliance command prompt as root.

2. Open the following file in a text editor.

   /etc/vcac/security.properties
3 Change consoleproxy.service.port from its default of 8444 to an unused port.
4 Save and close security.properties.
5 Restart the vRealize Automation appliance.

In an HA environment, make the same change to all vRealize Automation appliances.

**Change a vRealize Automation Appliance FQDN Back to the Original FQDN**

In some cases, a vRealize Automation appliance FQDN might change when you do not want it to. For example, the FQDN changes if you create an Integrated Windows Authentication (IWA) directory for a domain other than the domain that the appliance is on.

If you create an IWA directory for another domain, take the following steps to change the appliance FQDN back to the original FQDN.

**Procedure**

1. Log in to vRealize Automation and create the IWA directory as you normally would.
   See [Configure an Active Directory over LDAP/IWA Link](#).
2. If this is an HA environment, also follow the steps in [Configure Directories Management for High Availability](#).
3. Creating an IWA directory for a domain other than the one that an appliance is on silently changes the appliance FQDN.
   For example, va1.domain1.local changes to va1.domain2.local when you create an IWA directory for domain2.local.
   Undo the change by renaming each appliance back to its original FQDN. See the associated procedure under [Changing Host Names and IP Addresses](#).
4. After the appliances are completely back online with their original FQDN, log in to each IaaS node, and take the following steps.
   a. Open the following file in a text editor.
      C:\Program Files (x86)\VMware\vCAC\Management\Agent\VMware.IaaS.Management.Agent.exe.Config
   b. Change each appliance endpoint `address` FQDN back to the original FQDN.
      For example, from:

```xml
<endpoint address="https://va1.domain2.local:5480/"
   thumbprint="98C55BACEC53E31609EE1614CE4A8336848A0D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
   thumbprint="0468BF6EDBC6F2299BE810D07FD1094197E324ED" />
```
To:

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

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

6 Go to vRA settings > Messaging and click Reset RabbitMQ Cluster.

7 After the reset finishes, log in to each appliance management interface.

8 Go to vRA Settings > Cluster, and verify that all nodes are connected to the cluster.

**Configure SQL AlwaysOn Availability Group**

You must make configuration changes if you set up SQL AlwaysOn Availability Group (AAG) after installing vRealize Automation.

When setting up SQL AAG after installation, follow the steps in VMware Knowledge Base article 2074607 to configure vRealize Automation with the AAG listener FQDN as the SQL Server host.

**Add Network Interface Controllers After Installing vRealize Automation**

vRealize Automation supports multiple network interface controllers (NICs). After installation, you can add NICs to the vRealize Automation appliance or IaaS Windows server.

Multiple NICs might be needed for some vRealize Automation deployments, for example:

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

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

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

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

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

**Prerequisites**

Completely install vRealize Automation to your vCenter environment.
Procedure

1. In vCenter, add NICs to each vRealize Automation appliance.
   a. Right click the appliance and select Edit Settings.
   b. Add VMXNET3 NICs.
   c. If it is powered on, restart the appliance.

2. Log in to the vRealize Automation appliance management interface as root.
   https://vrealize-automation-appliance-FQDN:5480

3. Select Network, and verify that multiple NICs are available.

4. Select Address, and configure the IP address for the NICs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address Type</td>
<td>Static</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>172.22.0.2</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

5. Verify that all vRealize Automation nodes can resolve each other by DNS name.

6. Verify that all vRealize Automation nodes can access any load balanced FQDNs for vRealize Automation components.

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

8. In vCenter, add NICs to IaaS Windows servers.
   a. Right click the IaaS server and select Edit Settings.
   b. Add NICs to the IaaS server virtual machine.

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

What to do next

(Optional) If you need static routes, see Configure Static Routes.

Configure Static Routes

When adding NICs to a vRealize Automation installation, if you need static routes, you open a command prompt session to configure them.

Prerequisites

Add multiple NICs to vRealize Automation appliances or IaaS Windows servers.
Procedure

1. Log in to the vRealize Automation appliance command line as root.
2. Open the routes file in a text editor.
   
   /etc/sysconfig/network/routes

3. Locate the default line for the default gateway, but do not modify it.

   **Note** In cases where the default gateway needs to change, use the vRealize Automation management interface instead.

4. Below the default line, add new lines for static routes. For example:

   ```
   default 10.10.10.1 - -
   172.30.30.0 192.168.100.1 255.255.255.0 eth0
   192.168.210.0 192.168.230.1 255.255.255.0 eth2
   ```

5. Save and close the routes file.
6. Restart the appliance.
7. In HA clusters, repeat the process for each appliance.
8. Log in to the IaaS Windows server as an administrator.
9. Open a command prompt as administrator.
10. To configure a static route, enter the route -p add command, where -p persists the static route across restarts. For example:

    ```
    C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
    OK!
    ```

    For more information about configuring static routes in Windows, see the Microsoft documentation.

**Access Patch Management**

Technical support for your vRealize Automation installation might involve a software patch that you install or remove using the vRealize Automation appliance management interface.

The patch interface cannot patch the following vRealize Automation components.

- The Management Agent
- Non vSphere agents such as XenServer, VDI, or Hyper-V

**Prerequisites**

- Take snapshots of all nodes in your vRealize Automation installation.
- Verify that all nodes in your vRealize Automation installation are up and running.
If you attempt to install or remove a patch without all nodes running, the vRealize Automation appliance management interface might become unresponsive. If that happens, contact technical support. Do not attempt to manage patches through other means or use vRealize Automation until you resolve the issue.

- If your environment uses load balancers for HA, disable traffic to secondary nodes until after installing or removing patches.
- If installing a new patch, obtain the patch file and copy it to the file system available to the browser you use for the vRealize Automation appliance management interface.
- Check the VMware Knowledge Base for late breaking or newly released information about patches.

Open the Knowledge Base and enter vRealize Automation patching in the search box. For example, VMware Knowledge Base article 51708 is monitored and updated with the latest vRealize Automation 7.4 patch information.

**Procedure**

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

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

2. Click vRA Settings > Patches.

3. Under Patch Management, click the option that you need, and follow the prompts.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Patch</td>
<td>Install a new patch that you have downloaded.</td>
</tr>
<tr>
<td>Installed Patches</td>
<td>Add the most recently installed patch to newly added cluster nodes.</td>
</tr>
<tr>
<td>Rollback</td>
<td>Remove the most recently installed patch and roll vRealize Automation back to the previous patch level.</td>
</tr>
<tr>
<td>History</td>
<td>Inspect the list of installed and removed patches.</td>
</tr>
</tbody>
</table>

To enable or disable Patch Management, log in to the vRealize Automation appliance command prompt as root, and enter one of the following commands.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

**Install a New Patch**

You install new vRealize Automation patches through the vRealize Automation appliance management interface.

**Prerequisites**

Check prerequisites, and go to the patch management interface. See Access Patch Management.

**Procedure**

1. Click New Patch.
2 Click **Upload Patch**.

3 Find and select the patch file.

4 After the patch uploads, review the patch details.

5 If you have the wrong patch, cancel by clicking **Remove**. Otherwise, click **Install**.

6 Verify that you followed the prerequisites, and click **Install**.

   It might take several minutes to install the patch.

7 Click **Done**.

If patch installation fails, you can click **Retry** to try again, or **Remove** to cancel. Canceling rolls vRealize Automation back to the state it was in before you started patch installation.

**Install the Current Patch on New Nodes**

You can add the most recently installed vRealize Automation patch to newly added cluster nodes.

**Prerequisites**

Check prerequisites, and go to the patch management interface. See [Access Patch Management](#).

**Procedure**

1 Click **Installed Patches**.

2 Select the most recent patch.

3 Click **Install**.

4 Follow the prompts.

**Remove the Current Patch**

You can remove the most recently installed vRealize Automation patch and roll back to the previous patch.

**Prerequisites**

Go to the patch management interface. See [Access Patch Management](#).

**Procedure**

1 Click **Rollback**.

2 Select the most recent patch.

3 Click **Rollback**.

4 Follow the prompts.

**Configure Access to the Default Tenant**

You must grant your team access rights to the default tenant before they can begin configuring vRealize Automation.
The default tenant is automatically created when you configure single sign-on in the installation wizard. You cannot edit the tenant details, such as the name or URL token, but you can create new local users and appoint additional tenant or IaaS administrators at any time.

**Procedure**

1. Log in to vRealize Automation as the administrator of the default tenant.
   - Navigate to the vRealize Automation product interface.
     https://vrealize-automation-FQDN/vcac
   - Log in with the user name **administrator** and the password you defined for this user when you configured SSO.

2. Select **Administration > Tenants**.

3. Click the name of the default tenant, **vsphere.local**.

4. Click the **Local users** tab.

5. Create local user accounts for the vRealize Automation default tenant.
   - Local users are tenant-specific and can only access the tenant in which you created them.
   - Click the Add (+) icon.
   - Enter details for the user responsible for administering your infrastructure.
   - Click **Add**.
   - Repeat this step to add one or more additional users who are responsible for configuring the default tenant.

6. Click the **Administrators** tab.

7. Assign your local users to the tenant administrator and IaaS administrator roles.
   - Enter a username in the **Tenant administrators** search box and press Enter.
   - Enter a username in the **IaaS administrators** search box and press Enter.
   - The IaaS administrator is responsible for creating and managing your infrastructure endpoints in vRealize Automation. Only the system administrator can grant this role.

8. Click **Update**.

**What to do next**

Provide your team with the access URL and log in information for the user accounts you created so they can begin configuring vRealize Automation.

- Your tenant administrators configure settings such as user authentication, including configuring Directories Management for high availability. See Configuring Tenant Settings.
- Your IaaS administrators prepare external resources for provisioning. See External Preparations for Provisioning.
If you configured Initial Content Creation during the installation, your configuration administrator can request the Initial Content catalog item to quickly populate a proof of concept. For an example of how to request the item and complete the manual user action, see Scenario: Request Initial Content for a Rainpole Proof of Concept Deployment.

Troubleshooting a vRealize Automation Installation

vRealize Automation troubleshooting provides procedures for resolving issues you might encounter when installing or configuring vRealize Automation.

Default Log Locations

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

Note For log collection, consider taking advantage of the vRealize Automation and vRealize Orchestrator Content Packs for vRealize Log Insight. The Content Packs and Log Insight provide a consolidated summary of log events for components in the vRealize suite. For more information, visit the VMware Solution Exchange.

For the most recent log location list, see VMware Knowledge Base article 2141175.

Windows Logs

Use the following to find log files for Windows events.

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

Installation Logs

Installation logs are in the following locations.

<table>
<thead>
<tr>
<th>Log</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Logs</td>
<td>C:\Program Files (x86)\vCAC\InstallLogs</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log</td>
</tr>
<tr>
<td>WAPI Installation Logs</td>
<td>C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename,basename-{XXX}&lt;</td>
</tr>
</tbody>
</table>

IaaS Logs

IaaS logs are in the following locations.

<table>
<thead>
<tr>
<th>Log</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Logs</td>
<td>C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs</td>
</tr>
<tr>
<td>Repository Log</td>
<td>C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs</td>
</tr>
<tr>
<td>Manager Service Logs</td>
<td>C:\Program Files (x86)\VMware\vCAC\Server\Logs</td>
</tr>
</tbody>
</table>
Log | Default Location
---|------------------
DEM Orchestrator Logs | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name>\ DEO \Logs
Agent Logs | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

vRealize Automation Framework Logs

Log entries for vRealize Automation Frameworks are located in the following location.

Log | Default Location
---|------------------
Framework Logs | /var/log/vmware

Software Component Provisioning Logs

Software component provisioning logs are located in the following location.

Log | Default Location
---|------------------
Software Agent Bootstrap Log | /opt/vmware-appdirector (for Linux) or \opt\vmware-appdirector (for Windows)
Software Lifecycle Script Logs | /tmp/taskId (for Linux)
 | \Users\darwin\AppData\Local\Temp\taskId (for Windows)

Collection of Logs for Distributed Deployments

You can create a zip file that bundles all logs for components of a distributed deployment.

Rolling Back a Failed Installation

When an installation fails and rolls back, the system administrator must verify that all required files have been uninstalled before starting another installation. Some files must be uninstalled manually.

Roll Back a Minimal Installation

A system administrator must manually remove some files and revert the database to completely uninstall a failed vRealize Automation IaaS installation.

Procedure

1. If the following components are present, uninstall them with the Windows uninstaller.
   - vRealize Automation Agents
   - vRealize Automation DEM-Worker
   - vRealize Automation DEM-Orchestrator
   - vRealize Automation Server
vRealize Automation WAPI

**Note**  If you see the following message, restart the machine and then follow the steps in this procedure: Error opening installation log file. Verify that the specified log file location exists and it is writable

**Note**  If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.

2 Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.

3 In IIS (Internet Information Services Manager) select Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).

4 Check that the Applications Repository, vRealize Automation and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.

The installation is completely removed.

**Roll Back a Distributed Installation**

A system administrator must manually remove some files and revert the database to completely uninstall a failed IaaS installation.

**Procedure**

1 If the following components are present, uninstall them with the Windows uninstaller.

- vRealize Automation Server
- vRealize Automation WAPI

**Note**  If you see the following message, restart the machine and then follow this procedure: Error opening installation log file. Verify that the specified log file location exists and it is writable.

**Note**  If the Windows system has been reverted or you have uninstalled IaaS, you must run the `iisreset` command before you reinstall vRealize Automation IaaS.

2 Revert your database to the state it was in before the installation was started. The method you use depends on the original database installation mode.

3 In IIS (Internet Information Services Manager) select the Default Web Site (or your custom site) and click **Bindings**. Remove the https binding (defaults to 443).

4 Check that the Applications Repository, vCAC and WAPI have been deleted and that the application pools RepositoryAppPool, vCACAppPool, WapiAppPool have also been deleted.
Table 1-44. Roll Back Failure Points

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

Create a vRealize Automation Support Bundle

You can create a vRealize Automation support bundle using the vRealize Automation appliance management interface. Support bundles gather logs, and help you or VMware technical support to troubleshoot vRealize Automation problems.

Procedure

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

2. Log in as root, and click vRA Settings > Cluster.

3. Click Create Support Bundle.

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

Support bundles include information from the vRealize Automation appliance and IaaS Windows servers. If you lose connectivity between the vRealize Automation appliance and IaaS components, the support bundle might be missing the IaaS component logs.

To see which log files were collected, unzip the support bundle and open the Environment.html file in a Web browser. Without connectivity, IaaS components might appear in red in the Nodes table. Another reason that the IaaS logs are missing might be that the vRealize Automation management agent service has stopped on IaaS Windows servers that appear in red.

General Installation Troubleshooting

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Installation or Upgrade Fails with a Load Balancer Timeout Error

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

Problem

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.
Cause

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

Solution

1. Increase your load balancer timeout value to at least 100 seconds.
2. Rerun the installation or upgrade.

Server Times Are Not Synchronized

An installation might not succeed when IaaS time servers are not synchronized with the vRealize Automation appliance.

Problem

You cannot log in after installation, or the installation fails while it is completing.

Cause

Time servers on all servers might not be synchronized.

Solution

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

- Set a vRealize Automation appliance time source:
  a. Log in to the vRealize Automation appliance management interface as root.
     https://vrealize-automation-appliance-FQDN:5480
  b. Select Admin > Time Settings, and set the time synchronization source.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Time</td>
<td>Synchronize to the vRealize Automation appliance ESXi host.</td>
</tr>
<tr>
<td>Time Server</td>
<td>Synchronize to one external Network Time Protocol (NTP) server. Enter the FQDN or IP address of the NTP server.</td>
</tr>
</tbody>
</table>

- For IaaS Windows servers, see Enable Time Synchronization on the Windows Server.

Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7

When you use Internet Explorer 9 or 10 on Windows 7 and compatibility mode is enabled, some pages appear to have no content.

Problem

When using Internet Explorer 9 or 10 on Windows 7, the following pages have no content:

- Infrastructure
- Default Tenant Folder on the Orchestrator page
Server Configuration on the Orchestrator page

Cause

The problem could be related to compatibility mode being enabled. You can disable compatibility mode for Internet Explorer with the following steps.

Solution

Prerequisites

Ensure that the menu bar is displayed. If you are using Internet Explorer 9 or 10, press Alt to display the Menu bar (or right-click the Address bar and then select Menu bar).

Procedure

1. Select Tools > Compatibility View settings.
2. Deselect Display intranet sites in Compatibility View.
3. Click Close.

Cannot Establish Trust Relationship for the SSL/TLS Secure Channel

You might receive the message "Cannot establish trust relationship for the SSL/TLS secure channel when upgrading security certificates for vCloud Automation Center."

Problem

If a certificate issue occurs with vcac-config.exe when upgrading a security certificate, you might see the following message:

The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel

You can find more information about the cause of the issue by using the following procedure.

Solution

1. Open vcac-config.exe.config in a text editor, and locate the repository address:
   
   <add key="repositoryAddress" value="https://IaaS-address:443/repository/" />

2. Open Internet Explorer to the address.
3. Continue through any error messages about certificate trust issues.
4. Obtain a security report from Internet Explorer, and use it to troubleshoot why the certificate is not trusted.

If problems persist, repeat the procedure by browsing with the address that needs to be registered, the Endpoint address that you used to register with vcac-config.exe.

Connect to the Network Through a Proxy Server

Some sites might connect to the Internet through a proxy server.
Problem
Your deployment cannot connect to the open Internet. For example, you cannot access Web sites, public clouds that you manage, or vendor addresses from which you download software or updates.

Cause
Your site connects to the Internet through a proxy server.

Solution

Prerequisites
Obtain proxy server names, port numbers, and credentials from the administrator for your site.

Procedure
1. Open a Web browser to the vRealize Automation appliance management interface URL.
   https://vrealize-automation-appliance-FQDN:5480
2. Log in as root, and click Network.
3. Enter your site proxy server FQDN or IP address, and port number.
4. If your proxy server requires credentials, enter the user name and password.
5. Click Save Settings.

What to do next
Configuring to use a proxy might affect VMware Identity Manager user access. To correct the issue, see Proxy Prevents VMware Identity Manager User Log In.

Console Steps for Initial Content Configuration
There is an alternative to using the vRealize Automation installation interface to create the configuration administrator account and initial content.

Problem
As the last part of installing vRealize Automation, you follow the process to enter a new password, create the configurationadmin local user account, and create initial content. An error occurs, and the interface enters an unrecoverable state.

Solution
Instead of using the interface, enter console commands to create the configurationadmin user and initial content. Note that the interface might fail after successfully completing part of the process, so you might only need some of the commands.

For example, you might inspect logs and vRealize Orchestrator workflow execution, and determine that the interface-based setup created the configurationadmin user but not the initial content. In that case, you can enter just the last two console commands to complete the process.
Procedure

1. Log in to the vRealize Automation appliance console as root.

2. Import the vRealize Orchestrator workflow by entering the following command:

   `/usr/sbin/vcac-config -e content-import --
   workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
   workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --
   tenant $TENANT`

3. Execute the workflow to create the configurationadmin user:

   `/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
   password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-a824-1958d91efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD --
   tenant $TENANT`

4. Import the ASD blueprint by entering the following command:

   `/usr/sbin/vcac-config -e content-import --
   blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
   asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
   $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT`

5. Execute the workflow to configure initial content:

   `/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
   password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD`

**Cannot Downgrade vRealize Automation Licenses**

An error occurs when you submit the license key of a lower product edition.

**Problem**

You see the following message when using the vRealize Automation administration interface Licensing page to submit the key to a product edition that is lower than the current one. For example, you start with an enterprise license and try to enter an advanced license.

```plaintext
Unable to downgrade existing license edition
```

**Cause**

This vRealize Automation release does not support the downgrading of licenses. You can only add licenses of an equal or higher edition.

**Solution**

To change to a lower edition, reinstall vRealize Automation.
Troubleshooting the vRealize Automation Appliance

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using your vRealize Automation appliances.

Installers Fail to Download

Installers fail to download from the vRealize Automation appliance.

Problem

Installers do not download when running `setup_vrealize-automation-appliance-FQDN@5480.exe`.

Cause

- Network connectivity issues when connecting to the vRealize Automation appliance machine.
- Not able to connect to the vRealize Automation appliance machine because the machine cannot be reached or it cannot respond before the connection times out.

Solution

1. Verify that you can connect to the vRealize Automation URL in a Web browser.
   - `https://vrealize-automation-appliance-FQDN`
2. Check the other vRealize Automation appliance troubleshooting topics.
3. Download the setup file and reconnect to the vRealize Automation appliance.

Encryption.key File has Incorrect Permissions

A system error can result when incorrect permissions are assigned to the Encryption.key file for a virtual appliance.

Problem

You log in to vRealize Automation appliance and the Tenants page is displayed. After the page has begun loading, you see the message System Error.

Cause

The Encryption.key file has incorrect permissions or the group or owner user level is incorrectly assigned.

Solution

Prerequisites

Log in to the virtual appliance that displays the error.

Note If your virtual appliances are running under a load balancer, you must check each virtual appliance.
Procedure

1. View the log file `/var/log/vcac/catalina.out` and search for the message Cannot write to `/etc/vcac/Encryption.key`.

2. Go to the `/etc/vcac/` directory and check the permissions and ownership for the `Encryption.key` file. You should see a line similar to the following one:

   ```bash
   -rw------- 1 vcac vcac 48 Dec 4 06:48 encryption.key
   ```

   Read and write permission is required and the owner and group for the file must be `vcac`.

3. If the output you see is different, change the permissions or ownership of the file as needed.

What to do next

Log in to the Tenant page to verify that you can log in without error.

**Directories Management Identity Manager Fails to Start After Horizon-Workspace Restart**

In a vRealize Automation high availability environment, the Directories Management Identity Manager can fail to start after the horizon-workspace service is restarted.

**Problem**

The horizon-workspace service cannot start due an error similar to the following:

```plaintext
Error creating bean with name 'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
   Invocation of init method failed; nested exception is
   liquibase.exception.LockException: Could not acquire change log lock. Currently
   locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
   (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

**Cause**

The Identity Manager might fail to start in a high availability environment because of issues with the liquibase data management utility used by vRealize Automation.

**Solution**

1. Log in as root to a console session on the vRealize Automation appliance.

2. Stop the horizon-workspace service by entering the following command.

   ```bash
   #service horizon-workspace stop
   ```

3. Open the Postgres shell as super user.

   ```bash
   su postgres
   ```

4. Navigate to the correct bin directory.

   ```bash
   cd /opt/vmware/vpostgres/current/bin
   ```
5 Connect to the database.
   $ psql vcac

6 From saas.databasechangeloglock, run the following SQL query.
   $ select * from databasechangeloglock;
   If the output shows a value of "t" for true, the lock must be released manually.

7 If you need to manually release the lock, run the following SQL query.
   $ update saas.databasechangeloglock set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;

8 From saas.databasechangeloglock, run the following SQL query.
   $ select * from databasechangeloglock;
   The output should show a value of "f" for false, meaning it is unlocked.

9 Exit the Postgres vcac database.
   $ vcac=# \q

10 Close the Postgres shell.
    $ exit

11 Start the horizon-workspace service.
    $ #service horizon-workspace start

**Incorrect Appliance Role Assignments After Failover**

After a failover occurs, master and replica vRealize Automation appliance nodes might not have the correct role assignment, which affects all services that require database write access.

**Problem**

In a high availability cluster of vRealize Automation appliances, you shut down or make the master database node inaccessible. You use the management console on another node to promote that node as the new master, which restores vRealize Automation database write access.

Later, you bring the old master node back online, but the Database tab in its management console still lists the node as the master node even though it is not. Attempts to use any node management console to clear the problem by officially promoting the old node back to master fail.

**Solution**

When failover occurs, follow these guidelines when configuring old versus new master nodes.

- Before promoting another node to master, remove the previous master node from the load balancer pool of vRealize Automation appliance nodes.
To have vRealize Automation bring an old master node back to the cluster, let the old machine come online. Then, open the new master management console. Look for the old node listed as invalid under the Database tab, and click its Reset button.

After a successful reset, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.

To manually bring an old master node back to the cluster, bring the machine online, and join it to the cluster as if it were a new node. While joining, specify the newly promoted node as the primary node.

After successfully joining, you may restore the old node to the load balancer pool of vRealize Automation appliance nodes.

Until you correctly reset or rejoin an old master node to the cluster, do not use its management console for cluster management operations, even if the node came back online.

After you correctly reset or rejoin, you may promote an old node back to master.

**Failures After Promotion of Replica and Master Nodes**

A disk space issue, along with the promotion of replica and master vRealize Automation appliance database nodes, might cause provisioning problems.

**Problem**

The master node runs out of disk space. You log in to its management interface Database page, and promote a replica node with enough space to become the new master. Promotion appears to succeed when you refresh the management interface page, even though an error message occurred.

Later, on the node that was the old master, you free up the disk space. After you promote the node back to master, however, provisioning operations fail by being stuck IN_PROGRESS.

**Cause**

vRealize Automation cannot properly update the old master node configuration when the problem is not enough space.

**Solution**

If the management interface displays errors during promotion, temporarily exclude the node from the load balancer. Correct the node problem, for example by adding disk, before re-including it on the load balancer. Then, refresh the management interface Database page and verify that the right nodes are master and replica.

**Incorrect vRealize Automation Component Service Registrations**

The vRealize Automation appliance management interface can help you resolve registration problems with vRealize Automation component services.
Problem

Under normal operation, all vRealize Automation component services must be unique and in a REGISTERED state. Any other set of conditions might cause vRealize Automation to behave unpredictably.

Cause

The following are examples of problems that might occur with vRealize Automation component services.

- A service has become inactive.
- Server settings caused a service to be in a state other than REGISTERED.
- A dependency on another service caused a service to be in a state other than REGISTERED.

Solution

Re-register component services that appear to have problems.

1. Take a snapshot of the vRealize Automation appliance.
   You might need to revert to the snapshot if you try different service changes, and the appliance ends up in an unpredictable state.

2. Log in to the vRealize Automation appliance management interface as root.
   https://vrealize-automation-appliance-FQDN:5480

3. Click Services.

4. In the list of services, look for a service that is not in the correct state or has other problems.

5. If a faulty service is the iaas-service, go to the next step.
   Otherwise, to have vRealize Automation re-register the service, log in to a console session on the vRealize Automation appliance as root, and restart vRealize Automation by entering the following command.

   service vcac-server restart

   If there are services associated with the embedded vRealize Orchestrator instance, enter the following additional command.

   service vco-restart restart

6. If a faulty service is the iaas-service, take the following steps to re-register it.
   a. Do not unregister the service.
   b. On the primary IaaS Web Server, log in with an account that has Administrator rights.
   c. Open a command prompt as Administrator.
   d. Run the following command.
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v

The password is the administrator@vsphere.local password.

e) Run a command to update the registration information in the IaaS database.

SQL Server with Windows Authentication:

"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v

SQL Server with Native SQL Authentication:

"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -sp SQL-user-password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v

To find the server or database name, inspect the following file in a text editor, and search for repository. Data Source and Initial Catalog values reveal the server address and database name, respectively.

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

The SQL user must have DBO privileges on the database.

f) Register the endpoints by running the following commands:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN/vcac -- Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN/WAPI -- Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN/repository -- Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN/WAPI/api/status -- Endpoint status -v
```

g) Register catalog items by running the following command:

"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterCatalogTypesAsync -v

h) Restart IIS.

iisreset
i Log in to the primary IaaS Manager Service host.

j Restart the vRealize Automation Windows service.

To re-register any services associated with an external system, such as an external vRealize Orchestrator instance, log in to the external system and restart the services there.

Additional NIC Causes Management Interface Errors

After you add a second network interface card (NIC) to a vRealize Automation appliance, some vRealize Automation management interface pages fail to load properly.

Problem

You successfully add a second NIC using vCenter, and the following vRealize Automation management interface pages display errors instead of loading.

- The Network > Status page displays an error about an unresponsive script.
- The Network > Address page displays an error about failing to read network interface information.

Cause

Starting in version 7.3, the vRealize Automation appliance can support dual NICs. However, the engineering template on which the appliance is based prevents the management interface from working properly until you apply the solution.

Solution

After adding an additional NIC, restart the vRealize Automation appliance.

Cannot Promote a Secondary Virtual Appliance to Master

In vRealize Automation, low virtual appliance memory might prevent virtual appliance promotions in the cluster.

Problem

The master node runs low on memory. You log in to its management interface Database page, and try to promote a secondary node to become the new master. The following error occurs.

```plaintext
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

Cause

Promotion only succeeds when all nodes can confirm reconfiguration to a newly promoted master. The low memory prevents the old master from confirming, even though all nodes are reachable.
Solution

Power off the master node that has low memory. Log in to the secondary node management interface Database page, and promote the secondary node.

Active Directory Sync Log Retention Time Is Too Short

In vRealize Automation, the Active Directory Sync logs go back only a couple days.

Problem

After two days, Active Directory Sync logs disappear from the management interface. Folders for the logs also disappear from the following vRealize Automation appliance directory.

/db/elasticsearch/horizon/nodes/0/indices

Cause

To conserve space, vRealize Automation sets the maximum retention time for Active Directory Sync logs to three days.

Solution

1. Log in to a console session on the vRealize Automation appliance as root.
2. Open the following file in a text editor.
   
   /usr/local/horizon/conf/runtime-config.properties

3. Increase the analytics.maxQueryDays property.

4. Save and close runtime-config.properties.

5. Restart the identity manager and elastic search services.

   service horizon-workspace restart
   service elasticsearch restart

RabbitMQ Cannot Resolve Host Names

RabbitMQ uses short host names for vRealize Automation appliances by default, which might prevent nodes from resolving one another.

Problem

You try to join another vRealize Automation appliance to the cluster, and an error similar to the following occurs.

```bash
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS

attempted to contact: [rabbit@company]
```
rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
  - node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
  - home dir: /var/lib/rabbitmq
  - cookie hash: 4+kP1tKnxGyaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for details.

**Cause**

Your network configuration does not allow vRealize Automation appliances to resolve each other by short host name.

**Solution**

1. For all vRealize Automation appliances in the deployment, log in as root to a console session.
2. Stop the RabbitMQ service.
   
   ```
   service rabbitmq-server stop
   ```
3. Open the following file in a text editor.
   
   ```
   /etc/rabbitmq/rabbitmq-env.conf
   ```
4. Set the following property to true.
   
   ```
   USE_LONGNAME=true
   ```
5. Save and close `rabbitmq-env.conf`.
6. Reset RabbitMQ.
   
   ```
   vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
   ```
7. On just one vRealize Automation appliance node, run the following script.
   
   ```
   vcac-config cluster-config-ping-nodes --services rabbitmq-server
   ```
8. On all nodes, verify that the RabbitMQ service is started.
   
   ```
   vcac-vami rabbitmq-cluster-config get-rabbitmq-status
   ```

**Troubleshooting IaaS Components**

The troubleshooting topics for vRealize Automation IaaS components provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

**Prerequisite Fixer Cannot Install .NET Features**

The vRealize Automation Prerequisite Checker **Fix** option fails and displays messages about not finding the installation source for .NET 3.5.1.
Problem

The Prerequisite Checker needs to verify that .NET 3.5.1 is installed in order to satisfy requirements for Windows Server 2008 R2 systems with IIS 7.5, and Windows Server 2012 R2 systems with IIS 8.

Cause

For Windows Server 2012 R2, inability to connect to the Internet can prevent .NET automatic installation. Certain Windows 2012 R2 updates can also prevent installation. The problem occurs because the Windows version lacks a local copy of the .NET Framework 3.5 installation source.

Solution

Manually provide a .NET Framework 3.5 installation source.

2. In Server Manager, enable .NET Framework 3.5 by using the Add Roles and Features Wizard.
3. During the wizard, navigate to the .NET Framework 3.5 installation path on the ISO media.
4. After adding .NET Framework 3.5, rerun the vRealize Automation Prerequisite Checker.

Validating Server Certificates for IaaS

You can use the vcac-Config.exe command to verify that an IaaS server accepts vRealize Automation appliance and SSO appliance certificates.

Problem

You see authorization errors when using IaaS features.

Cause

Authorization errors can occur when IaaS does not recognize security certificates from other components.

Solution

1. Open a command prompt as an administrator and navigate to the Cafe directory at vra-installation-dir\Server\Model Manager Data\Cafe, typically C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe.
2. Type a command of the form
   
   
   Optional parameters are --su [SQL user name] and --sp [password].

   If the command succeeds you see the following message:

   | Certificates validated successfully. |
   | Command succeeded.                  |

   If the command fails, you see a detailed error message.

   **Note** This command is available only on the node for the Model Manager Data component.
Credentials Error When Running the IaaS Installer
When you install IaaS components, you get an error when entering your virtual appliance credentials.

Problem
After providing credentials in the IaaS installer, an org.xml.sax.SAXParseException error appears.

Cause
You used incorrect credentials or an incorrect credential format.

Solution
Ensure that you use the correct tenant and user name values.
For example, the SSO default tenant uses domain name such as vsphere.local, not administrator@vsphere.local.

Save Settings Warning Appears During IaaS Installation
Message appears during IaaS Installation. Warning: Could not save settings to the virtual appliance during IaaS installation.

Problem
An inaccurate error message indicating that user settings have not been saved appears during IaaS installation.

Cause
Communication or network problems can cause this message to appear erroneously.

Solution
Ignore the error message and proceed with the installation. This message should not cause the setup to fail.

Website Server and Distributed Execution Managers Fail to Install
Your installation of the vRealize Automation appliance infrastructure Web site server and distributed execution managers cannot proceed when the password for your IaaS service account contains double quotation marks.

Problem
You see a message telling you that installation of the vRealize Automation appliance distributed execution managers (DEMs) and Web site server has failed because of invalid msiexec parameters.

Cause
The IaaS service account password uses a double quotation mark character.
Solution

1. Verify that your IaaS service account password does not include double quotation marks as part of the password.
2. If your password contains double quotation marks, create a new password.
3. Restart the installation.

**IaaS Authentication Fails During IaaS Web and Model Management Installation**

When running the Prerequisite Checker, you see a message that the IIS authentication check has failed.

**Problem**

The message tells you that authentication is not enabled, but the IIS authentication check box is selected.

**Solution**

1. Clear the Windows authentication check box.
2. Click **Save**.
3. Select the Windows authentication check box.
4. Click **Save**.
5. Rerun the Prerequisite Checker.

**Failed to Install Model Manager Data and Web Components**

Your vRealize Automation installation can fail if the IaaS installer is unable to save the Model Manager Data component and Web component.

**Problem**

Your installation fails with the following message:

```markdown
The IaaS installer failed to save the Model Manager Data and Web components.
```

**Cause**

The failure has several potential causes.

- Connectivity issues to the vRealize Automation appliance or connectivity issues between the appliances. A connection attempt fails because there was no response or the connection could not be made.
- Trusted certificate issues in IaaS when using a distributed configuration.
- A certificate name mismatch in a distributed configuration.
- The certificate may be invalid or an error on the certificate chain might exist.
- The Repository Service fails to start.
- Incorrect configuration of the load balancer in a distributed environment.
Solution

- **Connectivity**
  
  Verify that you can connect to the vRealize Automation URL in a Web browser.

  https://vrealize-automation-appliance-FQDN

- **Trusted Certificate Issues**
  
  - In IaaS, open Microsoft Management Console with the command `mmc.exe` and check that the certificate used in the installation has been added to the Trusted Root Certificate Store in the machine.
  
  - From a Web browser, check the status of the MetaModel service and verify that no certificate errors appear:

    https://FQDN-or-IP/repository/data/MetaModel.svc

- **Certificate Name Mismatch**
  
  This error can occur when the certificate is issued to a particular name and a different name or IP address is used. You can suppress the certificate name mismatch error during installation by selecting **Suppress certificate mismatch**.

  You can also use the Suppress certificate mismatch option to ignore remote certificate revocation list match errors.

- **Invalid Certificate**
  
  Open Microsoft Management Console with the command `mmc.exe`. Check that the certificate is not expired and that the status is correct. Do this for all certificates in the certificate chain. You might have to import other certificates in the chain into the Trusted Root Certificate Store when using a Certificate hierarchy.

- **Repository Service**
  
  Use the following actions to check the status of the repository service.

  - From a Web browser, check the status of the MetaModel service:

    https://FQDN-or-IP/repository/data/MetaModel.svc

  - Check the Repository.log for errors.

  - Reset IIS (`iisreset`) if you have problems with the applications hosted on the Web site (Repository, vRealize Automation, or WAPI).

  - Check the Web site logs in `%SystemDrive%\inetpub\logs\LogFiles` for additional logging information.

  - Verify that Prerequisite Checker passed when checking the requirements.

  - On Windows 2012, check that WCF Services under .NET Framework is installed and that HTTP activation is installed.
IaaS Windows Servers Do Not Support FIPS

An installation cannot succeed when Federal Information Processing Standard (FIPS) is enabled.

Problem

Installation fails with the following error while installing the IaaS Web component.

This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

Cause

vRealize Automation IaaS is built on Microsoft Windows Communication Foundation (WCF), which does not support FIPS.

Solution

On the IaaS Windows server, disable the FIPS policy.

1. Go to Start > Control Panel > Administrative tools > Local Security Policy.
2. In the Group Policy dialog, under Local Policies, select Security Options.
3. Find and disable the following entry.

   System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

Adding an XaaS Endpoint Causes an Internal Error

When you attempt to create an XaaS endpoint, an internal error message appears.

Problem

Creation of an endpoint fails with the following internal error message, An internal error has occurred. If the problem persists, please contact your system administrator. When contacting your system administrator, use this reference: c0DD0C01. Reference codes are randomly generated and not linked to a particular error message.

Solution

1. Open the vRealize Automation appliance log file.

   /var/log/vcac/catalina.out

2. Locate the reference code in the error message.

   For example, c0DD0C01.

3. Search for the reference code in the log file to locate the associated entry.

4. Review the entries that appear above and below the associated entry to troubleshoot the problem.

   The associated log entry does not specifically call out the source of the problem.

Uninstalling a Proxy Agent Fails

Removing a proxy agent can fail if Windows Installer Logging is enabled.
Problem

When you try to uninstall a proxy agent from the Windows Control Panel, the uninstall fails and you see the following error:

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

Cause

This can occur if Windows Installer Logging is enabled, but the Windows Installer engine cannot properly write the uninstallation log file. For more information, see Microsoft Knowledge Base article 2564571.

Solution

1. Restart your machine or restart explorer.exe from the Task Manager.
2. Uninstall the agent.

Machine Requests Fail When Remote Transactions Are Disabled

Machine requests fail when Microsoft Distributed Transaction Coordinator (DTC) remote transactions are disabled on Windows server machines.

Problem

If you provision a machine when remote transactions are disabled on the Model Manager portal or the SQL Server, the request will not complete. Data collection fails and the machine request remains in a state of CloneWorkflow.

Cause

DTC Remote Transactions are disabled in the IaaS SQL Instance used by the vRealize Automation system.

Solution

1. Launch Windows Server Manager to enable DTC on all vRealize servers and associated SQL servers.

   In Windows 7, navigate Start > Administrative Tools > Component Services.

   Note  Ensure that all Windows servers have unique SIDs for MSDTC configuration.

   In addition, the IaaS Manager Service host must be able to resolve the NETBIOS name of the IaaS SQL Server database host. If it cannot resolve the NETBIOS name, add the SQL Server NETBIOS name to the Manager Service machine /etc/hosts file and restart the Manager Service.

2. Open all nodes to locate the local DTC, or the clustered DTC if using a clustered system.

   Navigate Component Services > Computers > My Computer > Distributed Transaction Coordinator.

3. Right click on the local or clustered DTC and select Properties.
Click the Security tab.

Select the **Network DTC Access** option.

Select the **Allow Remote Client** and **Allow Remote Administration** options.

Select the **Allow Inbound** and **Allow Outbound** options.

Enter or select NT AUTHORITY\Network Service in the **Account** field for the DTC Logon Account.

Click **OK**.

Remove machines that are stuck in the Clone Workflow state.

a Log in to the vRealize Automation product interface.

   https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name

b Navigate to **Infrastructure > Managed Machines**.

c Right click the target machine.

d Select **Delete** to remove the machine.

**Error in Manager Service Communication**

IaaS servers cloned from a template where DTC was already installed contain duplicate identifiers for DTC, which prevents communication among the nodes.

**Problem**

The IaaS Manager Service fails and posts the following error to the manager service log.

```
Communication with the underlying transaction manager has failed. --->
System.Runtime.InteropServices.COMException: The MSDTC transaction manager was
unable to pull the transaction from the source transaction manager due to
communication problems. Possible causes are: a firewall is present and it
doesn't have an exception for the MSDTC process, the two machines cannot
find each other by their NetBIOS names, or the support for network transactions
is not enabled for one of the two transaction managers.
```

**Cause**

When you clone an IaaS server that already has DTC installed, the clone contains the same unique identifier for DTC as the parent. Communication between the two machines fails.

**Solution**

1 On the clone, open a command prompt as Administrator.

2 Run the following command.

   ```
   msdtc -uninstall
   ```

3 Restart the clone.

4 Open another command prompt, and run the following command.

   ```
   msdtc -install manager-service-host-FQDN
   ```
Email Customization Behavior Has Changed

In vRealize Automation 6.0 or later, only notifications generated by the IaaS component can be customized by using the email template functionality from earlier versions.

Solution

You can use the following XSLT templates:

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

Email templates are located in the \Templates directory under the server installation directory, typically %SystemDrive%\Program Files x86\VMware\vCAC\Server. The \Templates directory also includes XSLT templates that are no longer supported and cannot be modified.

Troubleshooting Log-In Errors

The troubleshooting topics for log-in errors for vRealize Automation provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Attempts to Log In as the IaaS Administrator with Incorrect UPN Format Credentials Fails with No Explanation

You attempt to log in to vRealize Automation as an IaaS administrator and are redirected to the login page with no explanation.

Problem

If you attempt to log in to vRealize Automation as an IaaS administrator with UPN credentials that do not include the @yourdomain portion of the user name, you are logged out of SSO immediately and redirected to the login page with no explanation.
Cause

The UPN entered must adhere to a `youname.admin@yourdomain` format, for example if you log in using `j smith.admin@sqa.local` as the user name but the UPN in the Active Directory is only set as `j smith.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 `j smith.admin@sqa.local`. This information is provided in the log file in the `log/vcac` folder.

Log In Fails with High Availability

When you have more than one vRealize Automation appliance, the appliances must be able to identify each other by short hostname. Otherwise, you cannot log in.

Problem

You configure vRealize Automation for high availability by installing an additional vRealize Automation appliance. When you try to log in to vRealize Automation, a message about an invalid license appears. The message is incorrect though, because you determined that your license is valid.

Cause

The vRealize Automation appliance nodes do not correctly form a high availability cluster until they can resolve the short host names of the nodes in the cluster.

Solution

To allow a cluster of high availability vRealize Automation appliances to resolve short host names, take any of the following approaches. You must modify all appliances in the cluster.

Procedure

- Edit or create a search line in `/etc/resolv.conf`. The line should contain domains that hold vRealize Automation appliances. Separate multiple domains with spaces. For example:
  
  search sales.mycompany.com support.mycompany.com

- Edit or create domain lines in `/etc/resolv.conf`. Each line should contain a domain that holds vRealize Automation appliances. For example:
  
  domain support.mycompany.com

- Add lines to the `/etc/hosts` file so that each vRealize Automation appliance short name is mapped to its fully qualified domain name. For example:
  
  node1    node1.support.mycompany.com
  node2    node2.support.mycompany.com

Proxy Prevents VMware Identity Manager User Log In

Configuring to use a proxy might prevent VMware Identity Manager users from logging in.
Problem
You configure vRealize Automation to access the network through a proxy server, and VMware Identity Manager users see the following error when they attempt to log in.

Error Unable to get metadata

Solution
Prerequisites
Configure vRealize Automation to access the network through a proxy server. See Connect to the Network Through a Proxy Server.

Procedure
1. Log in to the console of the vRealize Automation appliance as root.
2. Open the following file in a text editor.
   /etc/sysconfig/proxy
3. Update the NO_PROXY line to ignore the proxy server for VMware Identity Manager logins.
   NO_PROXY=
   For example: NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"
4. Save and close proxy.
5. Restart the Horizon workspace service by entering the following command.
   service horizon-workspace restart

Upgrading vRealize Automation
You can upgrade your current vRealize Automation environment to the latest version.

Depending on your current vRealize Automation environment, you can upgrade to the latest version by performing an in-place upgrade or a side-by-side upgrade. Review the information on this page to determine the best upgrade method for your environment.

An in-place upgrade is a multi-step process. You perform procedures in a particular order to update the various components in your current environment. You must upgrade all product components to the same version. You can only perform an in-place upgrade for these paths.

- vRealize Automation 6.2.5 to 7.4
- vRealize Automation 7.1 to 7.4
- vRealize Automation 7.2 to 7.4
- vRealize Automation 7.3.x to 7.4
A side-by-side upgrade migrates the data in your current vRealize Automation environment to a target environment deployed with the latest version of vRealize Automation. You can perform a side-by-side upgrade for these paths.

- vRealize Automation 6.2.0 through 6.2.5 to 7.4
- vRealize Automation 7.0 and 7.0.1 to 7.4
- vRealize Automation 7.1, 7.2, and 7.3.x to 7.4

Migration does not change your current environment. If your current environment is integrated with vCloud Director, vCloud Air, or has physical endpoints, you must use migration to upgrade. Migration removes all unsupported endpoints and everything associated with them in the target environment.

Locate your current vRealize Automation version in this table. Use the documents on the right to perform an upgrade of your vRealize Automation environment to the latest version.

Table 1-45. Supported Upgrade Paths to vRealize Automation 7.4

<table>
<thead>
<tr>
<th>Your Currently Installed Version</th>
<th>Documentation for Incremental Upgrades</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation 7.1, 7.2, or 7.3.x</td>
<td>See one of these topics.</td>
</tr>
<tr>
<td></td>
<td>- Upgrading from vRealize Automation 7.1 or Greater to 7.4</td>
</tr>
<tr>
<td></td>
<td>- Migrating to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Automation 7.0 or 7.0.1</td>
<td>See Migrating to vRealize Automation 7.4.</td>
</tr>
<tr>
<td>vRealize Automation 6.2.5</td>
<td>See one of these topics.</td>
</tr>
<tr>
<td></td>
<td>- Upgrading vRealize Automation 6.2.5 to 7.4</td>
</tr>
<tr>
<td></td>
<td>- Migrating to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4</td>
<td>See Migrating to vRealize Automation 7.4</td>
</tr>
</tbody>
</table>

This table provides information about upgrading from an earlier vCloud Automation Center release. You must upgrade to vRealize Automation 6.2.5 before you upgrade to the latest version of vRealize Automation. You can find links to the documentation for 5.x and 6.x versions of vCloud Automation Center and vRealize Automation at https://www.vmware.com/support/pubs/vcac-pubs.html.

Table 1-46. Supported Upgrade Paths to vRealize Automation 6.2.5

<table>
<thead>
<tr>
<th>Your Currently Installed Version</th>
<th>Documentation for Incremental Upgrades</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center 6.0</td>
<td>Perform upgrades in the following order:</td>
</tr>
<tr>
<td>1 Upgrading vCloud Automation Center 6.0 to 6.0.1</td>
<td></td>
</tr>
<tr>
<td>2 Upgrading to vCloud Automation Center 6.1</td>
<td></td>
</tr>
<tr>
<td>3 Upgrading to vRealize Automation 6.2.x</td>
<td></td>
</tr>
<tr>
<td>vCloud Automation Center 6.0.1</td>
<td>Perform upgrades in the following order:</td>
</tr>
<tr>
<td>1 Upgrading to vCloud Automation Center 6.1</td>
<td></td>
</tr>
<tr>
<td>2 Upgrading to vRealize Automation 6.2.x</td>
<td></td>
</tr>
</tbody>
</table>
Table 1-46. Supported Upgrade Paths to vRealize Automation 6.2.5 (Continued)

<table>
<thead>
<tr>
<th>Your Currently Installed Version</th>
<th>Documentation for Incremental Upgrades</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center 6.1.x</td>
<td>Upgrading to vRealize Automation 6.2.x</td>
</tr>
<tr>
<td>vRealize Automation 6.2.x</td>
<td>Upgrade directly to the 6.2.5 release as described in Upgrading to vRealize Automation 6.2.x</td>
</tr>
</tbody>
</table>

**Note**  vCloud Automation Center rebranded to vRealize Automation in 6.2.0. Only the user interface and service names are changed. Directory names and program names that contain vcac are not affected.

If you are upgrading from a 6.2.x environment, review these items.

- The VMware vRealize Production Test Upgrade Assessment Tool analyzes your vRealize Automation 6.2.x environment for any feature configuration that can cause upgrade issues and checks that your environment is ready for upgrade. To download this tool and related documentation, go to the VMware vRealize Production Test Tool download product page.

- Upgrading from a 6.2.x environment to the latest version of vRealize Automation introduces many functional changes. For more information, see Considerations About Upgrading to This vRealize Automation Version.

- If you have customized your vRealize Automation 6.2.x deployment, contact your CCE support staff for additional information about upgrade considerations.

- Property dictionary controls that are not supported after upgrade can be restored using vRealize Orchestrator and property dictionary relationships.

- If you have workflows in your source environment that contain deprecated code, see the vRealize Automation Extensibility Migration Guide for information about the code changes required for conversion to event broker subscriptions.

To avoid a known problem when upgrading from vRealize Automation 6.2.0, perform the following steps on each IaaS Website node before you upgrade. This problem affects 6.2.0 only. Other 6.2.x versions are not affected.

1. Open Notepad with Administrative rights. In Start, right-click the Notepad icon and select **Run as administrator**.
2. Open the following file:
   
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\web.config

3. Locate the following statement in the file:
   
   <!-- add key="DisableMessageSignatureCheck" value="false"-->

4. Uncomment the statement and change the value from false to true.
   
   <add key="DisableMessageSignatureCheck" value="true" />

5. Save the file.

   If Notepad prompts you to **Save As**, you did not open Notepad as Administrator and must go back to step 1.
6. Open a Command Prompt with Administrative rights. In Start, right-click the Command Prompt icon and select **Run as administrator**.

7. Run reset.

8. Repeat steps 1–7 for all website nodes.

**Upgrading from vRealize Automation 7.1 or Greater to 7.4**

When you upgrade your vRealize Automation 7.1 or greater environment to the latest version, you use upgrade procedures specific to your 7.1 or greater environment.

This information is specific to upgrading vRealize Automation 7.1 or greater to 7.4. For information about other supported upgrade paths, see **Upgrading vRealize Automation**.

**Upgrading vRealize Automation 7.1, 7.2, or 7.3.x to 7.4**

You can upgrade of your current vRealize Automation 7.1, 7.2, or 7.3.x environment to 7.4. You use upgrade procedures specific to this version to upgrade your environment.

An in-place upgrade is a three-stage process. You upgrade the components in your current environment in this order.

1. vRealize Automation appliance
2. IaaS web server
3. vRealize Orchestrator

You must upgrade all product components to the same version.

Beginning with vRealize Automation 7.2, JFrog Artifactory Pro is no longer bundled with the vRealize Automation appliance. If you upgrade from an earlier version of vRealize Automation, the upgrade process removes JFrog Artifactory Pro. For more information, see Knowledge Base 2147237.

**Prerequisites for Upgrading vRealize Automation**

Before you run the upgrade your vRealize Automation 7.1, 7.2, or 7.3.x environment to 7.4, review these prerequisites.

**System Configuration Requirements**

Verify that the following prerequisites are finished before you begin an upgrade.

- Verify that all appliances and servers that are part of your deployment meet the system requirements for the latest version. See the **vRealize Automation Support Matrix** at VMware vRealize Automation Documentation.

- Consult the **VMware Product Interoperability Matrix** on the VMware website for information about compatibility with other VMware products.

- Verify that the vRealize Automation you are upgrading from is in stable working condition. Correct any problems before upgrading.

- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.
Hardware Configuration Requirements

Verify that the hardware in your environment is adequate for vRealize Automation 7.4.

See vRealize Automation Hardware Specifications and Capacity Maximums

Verify that the following prerequisites are finished before you begin an upgrade.

- You must have at least 18 GB RAM, 4 CPUs, Disk1=50 GB, Disk3=25 GB, and Disk4=50 GB before you run the upgrade.
  
  If the virtual machine is on vCloud Networking and Security, you might need to allocate more RAM space.
  
  Although general support for vCloud Networking and Security has ended, the VCNS custom properties continue to be valid for NSX purposes. See the Knowledge Base article 2144733.

- These nodes must have at least 5 GB of free disk space:
  - Primary IaaS Website
  - Microsoft SQL database
  - Model Manager

- The primary IaaS Website node where the Model Manager data is installed must have JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, you must set the JAVA_HOME environment variable to the new version.

- To download and run the upgrade, you must have the following resources:
  - At least 5 GB on the root partition
  - 5 GB on the /storage/db partition for the master vRealize Automation appliance
  - 5 GB on the root partition for each replica virtual appliance

- Check the /storage/log subfolder and remove any older archived ZIP files to clean up space.

General Prerequisites

Verify that the following prerequisites are finished before you begin an upgrade.

- You must install PowerShell 3.0 or above on your Windows IaaS systems before upgrading. The upgrade fails if PowerShell 3.0 or above is not installed.

- Perform an IISRESET on your IaaS Web and Manager Service machines if Microsoft IIS is installed. Performing the IISRESET verifies that there is not an IIS dependant service disabled in startup mode.

- If you use the DynamicTypes plugin, export the vRealize Orchestrator DynamicTypes plug-in configuration as a package.
  
    a. Log in to the Java Client as an administrator user.
    
    b. Select the Workflows tab.
    
    c. Select Library > Dynamic Types > Configuration.
    
    d. Select the Export Configuration as Package workflow and run it.
e Click **Not Set > Insert value.**

f Select the namespaces you want to export and click **Add** to add them to the package.

g Click **Submit** to export the package.

- You have access to all databases and all load balancers impacted by or participating in the vRealize Automation upgrade.
- You make the system unavailable to users while you perform the upgrade.
- You disable any applications that query vRealize Automation.
- Verify that Microsoft Distributed Transaction Coordinator (MSDTC) is enabled on all vRealize Automation and associated SQL servers. For instructions, see Knowledge Base article 2089503.

- Complete these steps if you are upgrading a distributed environment configured with an embedded PostgreSQL database.
  
a Examine the files in the *pgdata* directory on the master host before you upgrade the replica hosts.
  
b Navigate to the PostgreSQL data folder on the master host at */var/vmware/vpostgres/current/pgdata/.*
  
c Close any opened files in the *pgdata* directory and remove any files with a .swp suffix.
  
d Verify that all files in this directory have correct ownership: postgres:users.

In addition, verify that custom properties do not have spaces in their names. Before upgrading to this release of vRealize Automation, remove any space characters from your custom property names, for example replace the space with an underscore character, to allow the custom property to be recognized in the upgraded vRealize Automation installation. vRealize Automation custom property names cannot contain spaces. This issue can impact use of an upgraded vRealize Orchestrator installation that uses custom properties that contained spaces in earlier releases of either vRealize Automation or vRealize Orchestrator or both.

**Checklist for Upgrading vRealize Automation**

When you upgrade vRealize Automation 7.1, 7.2, or 7.3.x to 7.4, you update all vRealize Automation components in a specific order.

The order of upgrade varies depending on whether you are upgrading a minimal environment or a distributed environment with multiple vRealize Automation appliances.

Use the checklists to track your work as you complete the upgrade. Finish the tasks in the order they are given.
Table 1-47. Checklist for Upgrading a vRealize Automation Minimal Environment

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run NSX Network and Security Inventory Data Collection Before You</td>
<td>See Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.</td>
</tr>
<tr>
<td>Upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4. This</td>
<td></td>
</tr>
<tr>
<td>is only required when vRealize Automation is integrated with NSX.</td>
<td></td>
</tr>
<tr>
<td>Backup your current installation. This is a critical step.</td>
<td>For more information on how to back up and restore your system, see Back Up Your Existing vRealize</td>
</tr>
<tr>
<td></td>
<td>Automation Environment.</td>
</tr>
<tr>
<td></td>
<td>For general information, see Configuring Backup and Restore by Using Symantec Netbackup at</td>
</tr>
<tr>
<td>Download update to the vRealize Automation appliance.</td>
<td>See Downloading vRealize Automation Appliance Updates.</td>
</tr>
<tr>
<td>Install the update on the vRealize Automation appliance and IaaS</td>
<td>See Install the Update on the vRealize Automation Appliance and IaaS Components</td>
</tr>
<tr>
<td>components.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-48. Checklist for Upgrading a vRealize Automation Distributed Environment

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run NSX Network and Security Inventory Data Collection Before You</td>
<td>See Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.</td>
</tr>
<tr>
<td>Upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4. This</td>
<td></td>
</tr>
<tr>
<td>is only required when vRealize Automation is integrated with NSX.</td>
<td></td>
</tr>
<tr>
<td>Back up your current installation. This is a critical step.</td>
<td>For more information on how to back up and restore your system, see Back Up Your Existing vRealize</td>
</tr>
<tr>
<td></td>
<td>Automation Environment.</td>
</tr>
<tr>
<td></td>
<td>For detailed information, see Configuring Backup and Restore by Using Symantec Netbackup at</td>
</tr>
<tr>
<td>If you are upgrading from vRealize Automation 7.3.x, disable the</td>
<td>See Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.</td>
</tr>
<tr>
<td>PostgreSQL automatic failover.</td>
<td></td>
</tr>
<tr>
<td>Download updates to the vRealize Automation appliance.</td>
<td>See Downloading vRealize Automation Appliance Updates.</td>
</tr>
<tr>
<td>Disable your load balancer.</td>
<td>See your load balancer documentation.</td>
</tr>
<tr>
<td>Install the update on the master vRealize Automation appliance and</td>
<td>See Install the Update on the vRealize Automation Appliance and IaaS Components</td>
</tr>
<tr>
<td>IaaS components.</td>
<td></td>
</tr>
<tr>
<td>Note You must install the update on the master appliance in a</td>
<td></td>
</tr>
<tr>
<td>distributed environment.</td>
<td></td>
</tr>
<tr>
<td>Enable your load balancer.</td>
<td>Enable Your Load Balancers</td>
</tr>
</tbody>
</table>
vRealize Automation Environment User Interfaces
You use and manage your vRealize Automation environment with several interfaces.

User Interfaces
These tables describe the interfaces that you use to manage your vRealize Automation environment.

Table 1-49. vRealize Automation Administration Console

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Automation console for these system administrator tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>You must be a user with the system administrator role.</td>
</tr>
<tr>
<td>- Add tenants.</td>
<td>2 Click vRealize Automation console.</td>
<td></td>
</tr>
<tr>
<td>- Customize the vRealize Automation user interface.</td>
<td>You can also use this URL to open the vRealize Automation console: <a href="https://vra-va-hostname.domain.name/vcac">https://vra-va-hostname.domain.name/vcac</a></td>
<td></td>
</tr>
<tr>
<td>- Configure email servers.</td>
<td>3 Log in.</td>
<td></td>
</tr>
<tr>
<td>- View event logs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configure vRealize Orchestrator.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-50. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use vRealize Automation for these tasks.</td>
<td>1 Start a browser and enter the URL of your tenancy using the fully qualified domain name of the virtual appliance and the tenant URL name: <a href="https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name">https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name</a>.</td>
<td>You must be a user with one or more of these roles:</td>
</tr>
<tr>
<td>- Request new IT service blueprints.</td>
<td>2 Log in.</td>
<td>- Application Architect</td>
</tr>
<tr>
<td>- Create and manage cloud and IT resources.</td>
<td></td>
<td>- Approval Administrator</td>
</tr>
<tr>
<td>- Create and manage custom groups.</td>
<td></td>
<td>- Catalog Administrator</td>
</tr>
<tr>
<td>- Create and manage business groups.</td>
<td></td>
<td>- Container Administrator</td>
</tr>
<tr>
<td>- Assign roles to users.</td>
<td></td>
<td>- Container Architect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Health Consumer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Infrastructure Architect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Secure Export Consumer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software Architect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Tenant Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- XaaS Architect</td>
</tr>
<tr>
<td>Purpose</td>
<td>Access</td>
<td>Required Credentials</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>You use vRealize Automation Appliance Management for these tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>■ User name: root  ■ Password: Password you entered when you deployed the vRealize Automation appliance.</td>
</tr>
<tr>
<td>View the status of registered services.</td>
<td>2 Click vRealize Automation Appliance Management. You can also use this URL to open vRealize Automation Appliance Management: <a href="https://vra-va-hostname.domain.name:5480">https://vra-va-hostname.domain.name:5480</a>.</td>
<td></td>
</tr>
<tr>
<td>View system information and reboot or shutdown the appliance.</td>
<td>3 Log in.</td>
<td></td>
</tr>
<tr>
<td>Manage participation in the Customer Experience Improvement Program.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network status.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View update status and install updates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage administration settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage vRealize Automation host settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage SSO settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage product licenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the vRealize Automation Postgres database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure vRealize Automation messaging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure vRealize Automation logging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install IaaS components.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migrate from an existing vRealize Automation installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage IaaS component certificates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Xenon service.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-52. vRealize Orchestrator Client

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Orchestrator Client for these tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>You must be a user with the system administrator role or part of the vcoadmins group configured in the vRealize Orchestrator Control Center Authentication Provider settings.</td>
</tr>
<tr>
<td>Develop actions.</td>
<td>2 To download the client.jnlp file to your local computer, click vRealize Orchestrator Client.</td>
<td></td>
</tr>
<tr>
<td>Develop workflows.</td>
<td>3 Right-click the client.jnlp file and select Launch.</td>
<td></td>
</tr>
<tr>
<td>Manage policies.</td>
<td>4 On the Do you want to Continue? dialog box, click Continue.</td>
<td></td>
</tr>
<tr>
<td>Install packages.</td>
<td>5 Log in.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-53. vRealize Orchestrator Control Center

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the vRealize Orchestrator Control Center to edit the configuration of the default vRealize Orchestrator instance that is embedded in vRealize Automation. | 1. Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.  
2. Click vRealize Automation Appliance Management.  
You can also use this URL to open vRealize Automation Appliance Management: https://vra-va-hostname.domain.name:5480.  
3. Log in.  
4. Click vRA Settings > Orchestrator.  
5. Select Orchestrator user interface.  
6. Click Start.  
7. Click the Orchestrator user interface URL.  
8. Log in.                                                      | User Name  
- Enter root if role-based authentication is not configured.  
- Enter your vRealize Automation user name if it is configured for role-based authentication.  
Password  
- Enter the password you entered when you deployed the vRealize Automation appliance if role-based authentication is not configured.  
- Enter the password for your user name if your user name is configured for role-based authentication. |

### Table 1-54. Linux Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the Linux command prompt on a host, such as the vRealize Automation appliance host, for these tasks.  
- Stop or start services  
- Edit configuration files  
- Run commands  
- Retrieve data                                                     | 1. On the vRealize Automation appliance host, open a command prompt.  
One way to open the command prompt on your local computer is to start a session on the host using an application such as PuTTY.  
2. Log in.                                                      | User name: root  
Password: Password you created when you deployed the vRealize Automation appliance. |

### Table 1-55. Windows Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You can use a Windows command prompt on a host, such as the IaaS host, to run scripts. | 1. On the IaaS host, log in to Windows.  
One way to log in from your local computer is to start a remote desktop session.  
2. Open the Windows command prompt.  
One way to open the command prompt is to right-click the Start icon on the host and select Command Prompt or Command Prompt (Admin). | User name: User with administrative privileges.  
Password: User's password. |
Upgrading VMware Products Integrated with vRealize Automation

You must manage any VMware products integrated with your vRealize Automation environment when you upgrade vRealize Automation.

If your vRealize Automation environment is integrated with one or more additional products, you should upgrade vRealize Automation before you update the additional products. If vRealize Business for Cloud is integrated with vRealize Automation, you must unregister vRealize Business for Cloud before you upgrade vRealize Automation.

Follow the suggested workflow for managing integrated products when you upgrade vRealize Automation.

1. Upgrade vRealize Automation.
2. Upgrade VMware vRealize Operations Manager.
3. Upgrade VMware vRealize Log Insight.

This section provides additional guidance for managing vRealize Business for Cloud when it is integrated with your vRealize Automation environment.

Upgrading vRealize Operations Manager Integrated with vRealize Automation

Upgrade vRealize Operations Manager after you upgrade vRealize Automation.

Procedure
1. Upgrade vRealize Automation.
2. Upgrade vRealize Operations Manager. For information, see Updating Your Software in the VMware vRealize Operations Manager Documentation.

Upgrading vRealize Log Insight Integrated with vRealize Automation

Upgrade vRealize Log Insight after you upgrade vRealize Automation.

Procedure
1. Upgrade vRealize Automation.
2. Upgrade vRealize Log Insight. For information, see Upgrading vRealize Log Insight in the VMware vRealize Log Insight Documentation.

Upgrading vRealize Business for Cloud Integrated with vRealize Automation

When you upgrade your vRealize Automation environment, you must unregister and register your connection to vRealize Business for Cloud.

Perform this procedure to ensure continuity of service with vRealize Business for Cloud when you upgrade your vRealize Automation environment.

Upgrade vRealize Automation.

If necessary, upgrade vRealize Business for Cloud. See Upgrading vRealize Business for Cloud in the VMware vRealize Business for Cloud Documentation.

Register vRealize Business for Cloud with vRealize Automation. See Register vRealize Business for Cloud with vRealize Automation in the VMware vRealize Business for Cloud Documentation.

Preparing to Upgrade vRealize Automation

Complete these tasks before you upgrade vRealize Automation 7.1, 7.2, or 7.3.x to 7.4.

Complete these tasks in the order they appear in the checklist. See Checklist for Upgrading vRealize Automation.

Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation

Before you upgrade vRealize Automation 7.1, 7.2, or 7.3.x to 7.4, you must run NSX Network and Security Inventory data collection in your vRealize Automation 7.1, 7.2, or 7.3.x environment.

This data collection is necessary for the load balancer reconfigure action to work in vRealize Automation 7.4 for 7.1, 7.2, or 7.3.x deployments.

Procedure

- Run NSX Network and Security Inventory data collection on vRealize Automation 7.1, 7.2, or 7.3.x before you upgrade to 7.4. See Start Endpoint Data Collection Manually.

What to do next

Backup Prerequisites for Upgrading vRealize Automation 7.1, 7.2, or 7.3 to 7.4.

Backup Prerequisites for Upgrading vRealize Automation 7.1, 7.2, or 7.3 to 7.4

Complete the backup prerequisites before you begin your upgrade.

Prerequisites

- Verify that your source environment is fully installed and configured.
- Log in to your vSphere client and for each appliance in your source environment, back up all the vRealize Automation appliance configuration files in the following directories:
  - /etc/vcac/
  - /etc/vco/
  - /etc/apache2/
Back up the IaaS Microsoft SQL Server database. For information, find articles on the Microsoft Developer Network about creating a full SQL Server database backup.

Back up any files you have customized, such as DataCenterLocations.xml.

Create a snapshot of each virtual appliance and IaaS server. Adhere to regular guidelines for backing up the entire system in case vRealize Automation upgrade is unsuccessful. See Backup and Recovery for vRealize Automation Installations.

**Back Up Your Existing vRealize Automation Environment**

Before you upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4, shut down and take a snapshot of each vRealize Automation IaaS server on each Windows node and each vRealize Automation appliance on each Linux node. If an update is unsuccessful, use the snapshot to return to the last known good configuration and attempt another upgrade.

For information about starting vRealize Automation, see Start Up vRealize Automation.

**Prerequisites**

- Backup Prerequisites for Upgrading vRealize Automation 7.1, 7.2, or 7.3 to 7.4.

Beginning with vRealize Automation 7.0, the PostgreSQL database is always configured in high-availability mode. Log in to the vRealize Automation appliance management console and select vRA settings > Database to locate the current Master node. If the database configuration is listed as an external database, create a manual backup of this external database.

If the vRealize Automation Microsoft SQL database is not hosted on the IaaS server, create a database backup file.

Verify that you have completed the backup prerequisites for upgrading.

Verify that you have taken a snapshot of your system while it is shut down. This is the preferred method of taking a snapshot. See your vSphere 6.0 Documentation.

**Note**  When you back up the vRealize Automation appliance and the IaaS components, disable in-memory snapshots and quiesced snapshots.

- If you modified the app.config file, make a backup of that file. See Restore Changes to Logging in the app.config File.

- Make a backup of the external workflow configuration (xml/db) files. See Restore External Workflow Timeout Files.

- Verify that you have a location outside your current folder where you can store your backup file. See Backup Copies of .xml Files Cause the System to Time Out.

**Procedure**

1. Log in to your vSphere client.
2 Locate each vRealize Automation IaaS Windows machine, and each vRealize Automation appliance node.

3 To preserve data integrity you must shut down in a specific order. If you are using vCenter Server to manage your virtual machines, use the guest shutdown command to shut down vRealize Automation. See Shut Down vRealize Automation and follow the specified order.

4 Take a snapshot of each vRealize Automation machine.

5 Use your preferred backup method to create a full backup of each appliance node.

6 When you start vRealize Automation from the beginning, such as after a power outage, a controlled shutdown or after recovery, you must start the components in a specified order. For information, see Start Up vRealize Automation.

7 Log in to each vRealize Automation appliance management console and verify that the system is fully functional.
   a Click Services.
   b Verify that each service is REGISTERED.

What to do next

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous

If you upgrade from a distributed vRealize Automation environment that operates in PostgreSQL synchronous replication mode, you must change it to asynchronous before you upgrade.

Prerequisites

- You have a distributed vRealize Automation environment that you want to upgrade.
- You are logged in as root to vRealize Automation Appliance Management at https://vra-vahostname.domain.name:5480.

Procedure

1 Click vRA Settings > Database.

2 Click Async Mode and wait until the action completes.

3 Verify that all nodes in the Sync State column display Async status.

What to do next

Downloading vRealize Automation Appliance Updates

Downloading vRealize Automation Appliance Updates

You can check for updates on your appliance management console, and download the updates using one of the following methods.

For best upgrade performance, use the ISO file method.
To avoid potential problems when upgrading your appliance, or if issues arise during appliance upgrade, see VMware Knowledge Base article vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database (54987).

**Download Virtual Appliance Updates for Use with a CD-ROM Drive**

You can update your virtual appliance from an ISO file that the appliance reads from the virtual CD-ROM drive. This is the preferred method.

You download the ISO file and set up the primary appliance to use this file to upgrade your appliance.

**Prerequisites**

- Back up your existing vRealize Automation environment.
- Verify that all CD-ROM drives you use in your upgrade are enabled before you update a vRealize Automation appliance. See the vSphere documentation for information about adding a CD-ROM drive to a virtual machine in the vSphere client.

**Procedure**

1. Download the update repository ISO file.
   b. Click vRealize Automation Download Resources to go to the VMware download page.
   c. Download the appropriate file.
2. Locate the downloaded file on your system to verify that the file size is the same as the file on the VMware download page. Use the checksums provided on the download page to validate the integrity of your downloaded file. For information, see the links at the bottom of the VMware download page.
3. Verify that your primary virtual appliance is powered on.
4. Connect the CD-ROM drive for the primary virtual appliance to the ISO file you downloaded.
5. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
6. Click the Update tab.
7. Click Settings.
8. Under Update Repository, select Use CDROM Updates.
9. Click Save Settings.

**Download vRealize Automation Appliance Updates from a VMware Repository**

You can download the update for your vRealize Automation appliance from a public repository on the vmware.com website.

**Prerequisites**

- Back up your existing vRealize Automation environment.
Verify that your vRealize Automation appliance is powered on.

Procedure

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
2. Click the Update tab.
3. Click Settings.
4. (Optional) Set how often to check for updates in the Automatic Updates panel.
5. Select Use Default Repository in the Update Repository panel.
   - The default repository is set to the correct VMware.com URL.
6. Click Save Settings.

Updating the vRealize Automation Appliance and IaaS Components

After you finish the upgrade prerequisites and download the virtual appliance update, you install the update on the vRealize Automation 7.1, 7.2, or 7.3.x appliance to upgrade to 7.4.

For a minimal environment, you install the update on the vRealize Automation appliance. For a distributed environment, you install the update on the master appliance node. The time required for the update to finish varies according to your environment and network. When the update finishes, the system displays the changes made on the Update Status page of vRealize Automation Appliance Management. When the appliance update finishes, you must reboot the appliance. When you reboot the master appliance in a distributed environment, the system reboots each replica node.

After you reboot, Waiting for VA services to start appears on the Update Status page. The IaaS upgrade starts when the system is fully initialized and all services are running. You can observe the IaaS upgrade progress on the Update Status page. The first IaaS server component can take about 30 minutes to finish. During the upgrade, you see a message similar to Upgrading server components for node web1-vra.mycompany.com.

At the end of the upgrade process for each Manager Service node, you see a message similar to Enabling ManagerService automatic failover mode for node mgr-vra.mycompany.com. Beginning with vRealize Automation 7.3, the active Manager Service node changes from a manual election to a system decision about which node becomes the failover server. The system enables this feature during upgrade. If you have problems with this feature, see Update Fails to Upgrade the Management Agent.

Install the Update on the vRealize Automation Appliance and IaaS Components

You install the update on the vRealize Automation 7.1, 7.2, or 7.3.x virtual appliance to upgrade vRealize Automation and the IaaS components to 7.4.

Do not close the management console while you install the update.
If you encounter any problems during the upgrade process, see Troubleshooting the vRealize Automation Upgrade.

**Note** While upgrading the Management Agent on the IaaS virtual machines, a VMware public certificate is temporarily installed in your Trusted Publishers certificate store. The Management Agent upgrade process uses a PowerShell script that is signed with this certificate. When the upgrade is finished, this certificate is removed from your certificate store.

**Prerequisites**

- Verify that you selected a download method and completed the procedure for the method. See Downloading vRealize Automation Appliance Updates.
- For all high-availability environments, see Back Up Your Existing vRealize Automation Environment.
- For environments with load balancers, verify that you disabled all the redundant nodes and removed the health monitors. For information, see your load balancer documentation.
  - vRealize Automation appliance
  - IaaS Website
  - IaaS Manager Service
- For environments with load balancers, verify that the traffic is directed only to the primary node.
- Verify that the IaaS service hosted in Microsoft Internet Information Services (IIS) is running by performing the following steps:
  a. Start a browser and enter the URL `https://webhostname/Repository/Data/MetaModel.svc` to verify that the Web Repository is running. If successful, no errors are returned and you see a list of models in XML format.
  b. Log in to the IaaS Website and check that the status recorded in the `Repository.log` file reports OK. The file is located in the VCAC home folder at `/Server/Model Manager Web/Logs/Repository.log`.
    **Note** For a distributed IaaS Website, log in to the secondary website, without MMD, and stop Microsoft IIS temporarily. To ensure that the load balancer traffic is only going through the primary Web node, check the MetaModel.svc connectivity, and restart the Microsoft IIS.
- Verify that all IaaS nodes are in a healthy state by performing the following steps:
  a. On the primary virtual appliance, log in to vRealize Automation Appliance Management as `root` using the password you entered when you deployed the vRealize Automation appliance.
  b. Select vRA settings > Cluster.
  c. Under Last Connected, verify the following.
    - The IaaS nodes in the table have a last connected time of less than 30 seconds.
    - The virtual appliance nodes have a last connected time of less than 10 minutes.
If the IaaS nodes are not in communication with the vRealize Automation appliance, the upgrade fails.

To diagnose connectivity problems between the Management Agent and virtual appliance, perform these steps.

1. Log in to each IaaS node that is not listed or has a **Last Connected** time greater than 30 seconds.
2. Check the Management Agent logs to see if any errors are recorded.
3. If the Management Agent is not running, restart the agent in the Services console.

Note any orphaned nodes listed in the table. An orphaned node is a duplicate node that is reported on the host but does not exist on the host. You must delete all orphaned nodes. For more information, see Delete Orphaned Nodes on vRealize Automation.

- If you have a replica virtual appliance that is no longer part of the cluster, you must delete it from the cluster table. If you do not delete this appliance, the upgrade process displays a warning message that the replica update is unsuccessful.
- Verify that all saved and in-progress requests have finished successfully before you upgrade.
- If you upgrade the IaaS components manually after you update the vRealize Automation 7.1, 7.2, or 7.3.x appliance, see Exclude IaaS Upgrade. If you plan to upgrade IaaS manually, you must also stop all IaaS services, except Management Agent, on each IaaS node.

**Procedure**

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as **root** using the password you entered when you deployed the vRealize Automation appliance.
   
   For a distributed environment, open the management console on the master appliance.

2. Click **Services** and verify that all services are registered.

3. Select **vRA Settings > Database** and verify that this appliance is the master vRealize Automation appliance.
   
   You install the update only on the master vRealize Automation appliance. Each replica vRealize Automation appliance is updated with the master appliance.

4. Select **Update > Status**.

5. Click **Check Updates** to verify that an update is accessible.

6. (Optional) For instances of vRealize Automation appliance, click **Details** in the Appliance Version area to see information about the location of release notes.

7. Click **Install Updates**.
8 Click **OK**.

A message stating that the update is in progress appears. The system shows changes made during an upgrade on the Update Summary page. The time required for the update to finish varies according to your environment and network.

9 **(Optional)** To monitor the update in greater detail, use a terminal emulator to log in to the primary appliance. View the `updatecli.log` file at `/opt/vmware/var/log/vami/updatecli.log`. Additional upgrade progress information can also be seen in these files.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

If you log out during the upgrade process, you can continue to follow the update progress in the log file. The `updatecli.log` file might display information about the version of vRealize Automation that you are upgrading from. This displayed version changes to the proper version later in the upgrade process.

10 When the vRealize Automation appliance update finishes, click **System > Reboot** in the management console.

In a distributed environment, all successfully upgraded replica appliance nodes reboot when you reboot the master appliance.

The IaaS update starts when the system is initialized and all services are up and running. Click **Update > Status** to observe the IaaS upgrade progress.

11 When the IaaS update finishes, click **Cluster** in the appliance management console and verify that the version number is the current version for all IaaS nodes and components.

12 Click the **Telemetry** in the appliance management console. Read the note about participation in the Customer Experience Improvement Program (CEIP) and select to join or not join the program.

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

For more information about the Customer Experience Improvement Program, see [Join or Leave the Customer Experience Improvement Program for vRealize Automation](#).

**What to do next**

If your deployment uses a load balancer, perform these steps.

1 Enable the load balancer vRealize Automation health checks.
2 Re-enable the load balancer traffic for all vRealize Automation nodes.

If the IaaS components fail to upgrade, see [Upgrading the IaaS Server Components Separately If the Update Process Fails](#).
Upgrading the IaaS Server Components Separately If the Update Process Fails

If the automatic update process fails, you can upgrade the IaaS components separately.

If the vRealize Automation IaaS Web site and Manager Service successfully upgraded, you can run the IaaS upgrade shell script again without reverting to the snapshots you took before the upgrade. Sometimes a pending reboot event generated while upgrading multiple IaaS components installed on the same virtual machine can fail the upgrade. In this case, try manually rebooting the IaaS node and rerunning the upgrade to fix the problem. If the upgrade fails consistently, contact VMware support or attempt a manual upgrade by following these steps.

1. Revert your vRealize Automation appliance to its pre-update state.
2. Run a command to exclude the IaaS components from the update process. See Exclude IaaS Upgrade.
3. Run the update process on the vRealize Automation appliance.
4. Update the IaaS components separately using the Upgrade Shell Script or the vRealize Automation 7.4 IaaS installer msi package.

Upgrade IaaS Components Using the Upgrade Shell Script After Upgrading the vRealize Automation Appliance

Use the upgrade shell script to upgrade the IaaS components after you update each vRealize Automation 7.1, 7.2, or 7.3.x appliance to 7.4.

The updated vRealize Automation appliance contains a shell script that you use to upgrade each IaaS node and component.

You can run the upgrade script by using the vSphere console for the virtual machine or by using an SSH console session. If you use the vSphere console, you avoid intermittent network connectivity problems that can break the execution of the script.

If you stop the script while it is upgrading a component, the script stops when it finishes upgrading the component. If other components on the node still must be upgraded, you can run the script again.

When the upgrade finishes, you can review the upgrade result by opening the upgrade log file at /opt/vmware/var/log/vami/upgrade-iaas.log.

Prerequisites

- Review Troubleshooting the vRealize Automation Upgrade.
- Verify the successful update of all vRealize Automation appliances.
- If you reboot an IaaS server after you update all the vRealize Automation appliances but before you upgrade the IaaS components, stop all the IaaS services on Windows, except for the Management Agent service.
Before you run the upgrade shell script on the master vRealize Automation appliances node, click the **Services** on the appliance management console. Verify that each service, except for iaas-service, is **REGISTERED**.

To install the IaaS Management Agent manually on each IaaS node, finish these steps.

a. On the Open a browser and navigate to the VMware vRealize Automation IaaS Installation page on the appliance at https://virtual_appliance_host_FQDN:5480/installer.

b. Download the Management Agent installer, vCAC-IaaSManagementAgent-Setup.msi.

c. Log in to each vRealize Automation IaaS machine and upgrade the Management Agent with the Management Agent installer. Restart the Windows Management Agent service.

Verify that your primary IaaS Website and Model Manager node has JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, you must set the environment variable, JAVA_HOME, to the new version on each server node.

Log in to each IaaS Website node and verify that the creation date is earlier than the modified date in the web.config file. If the creation date for the web.config file is the same as or later than the modified date, perform the procedure in Upgrade Fails for IaaS Website Component.

To verify that each IaaS node has an upgraded IaaS Management Agent, perform these steps on each IaaS node:

a. Log in to the vRealize Automation appliance management console.

b. Select **vRA Settings > Cluster**.

c. Expand the list of all installed components on each IaaS node, and locate the IaaS Management Agent.

d. Verify that the Management Agent version is current.

Exclude IaaS Upgrade.

Verify that the IaaS Microsoft SQL Server database backup is accessible in case you must roll back.

Verify that snapshots of the IaaS servers in your deployment are available.

If the upgrade is unsuccessful, return to the snapshot and database backup and attempt another upgrade.

**Procedure**

1. Open a new console session on the vRealize Automation appliance host. Log in with the root account.

2. Change directories to /usr/lib/vcac/tools/upgrade/.

   It is important that all IaaS Management Agents are upgraded and healthy before running the ./upgrade shell script. If any IaaS Management Agent has a problem when you run the upgrade shell script, see Update Fails to Upgrade the Management Agent.
3 Run the upgrade script.
   a  At the command prompt, enter `./upgrade`.
   b  Press Enter.

For a description of the IaaS upgrade process, see Updating the vRealize Automation Appliance and IaaS Components.

If the Upgrade Shell Script is unsuccessful, review the `upgrade-iaas.log` file.

You can run the upgrade script again after you fix a problem.

What to do next
1 Restore Access to the Built-In vRealize Orchestrator Control Center.
2 If your deployment uses a load balancer, re-enable the vRealize Automation health monitors and the traffic to all nodes.

   For more information, see vRealize Automation Load Balancing.

Upgrading IaaS Components Using the IaaS Installer Executable File After Upgrading the vRealize Automation Appliance

You can use this alternative method to upgrade IaaS components after you upgrade the vRealize Automation 7.1, 7.2, or 7.3.x appliance to 7.4.

Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance

After you upgrade the vRealize Automation appliance to 7.4, download the IaaS installer to the machine where the IaaS components to be upgraded are installed.

If you see certificate warnings during this procedure, you can ignore them.

**Note**  Except for a passive backup instance of the Manager Service, the startup type for all services must be set to Automatic during the upgrade process. The upgrade process fails if you set services to Manual.

Prerequisites
- Verify that Microsoft .NET Framework 4.5.2 or later is installed on the IaaS installation machine. You can download the .NET installer from the vRealize Automation installer Web page. If you update .NET to 4.5.2 after you shut down the services and the machine restarted as part of the installation, you must manually stop all IaaS services except the Management agent.
- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. Enter `res://iesetup.dll/SoftAdmin.htm` in the search bar and press Enter.
- Log in as a local administrator to the Windows server where one or more of the IaaS components you want to upgrade are installed.

Procedure
1 Start a Web browser.
2 Enter the URL for the Windows installer download page.
   For example, https://vcac-va-hostname.domain.name:5480/installer, where vcac-va-hostname.domain.name is the name of the primary (master) vRealize Automation appliance node.

3 Click the IaaS installer link.

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

What to do next

Upgrade the IaaS Components After Upgrading vRealize Automation 7.1 or 7.2 to 7.3.

Upgrade the IaaS Components After Upgrading vRealize Automation 7.1 or 7.2 to 7.3

You must upgrade the SQL database and configure all systems that have IaaS components installed. You can use these steps for minimal and distributed installations.

Note The IaaS installer must be on the machine that contains the IaaS components you want to upgrade. You cannot run the installer from an external location, except for the Microsoft SQL database which also can be upgraded remotely from the Web node.

Verify that snapshots of the IaaS servers in your deployment are available. If the upgrade fails, you can return to the snapshot and attempt another upgrade.

Perform the upgrade so that services are upgraded in the following order:

1 IaaS Web sites
   If you are using a load balancer, disable traffic to all non-primary nodes.

   Finish the upgrade on one server before upgrading the next server that is running a Website service. Start with the one that has the Model Manager Data component installed.

   If you are performing a manual external Microsoft SQL database upgrade, you must upgrade the external SQL before you upgrade the Web node. You can upgrade the external SQL remotely from the Web node.

2 Manager Services
   Upgrade the active Manager Service before you upgrade the passive Manager Service.

   If you do not have SSL encryption enabled in your SQL instance, uncheck the SSL encryption checkbox in the Iaas Upgrade configuration dialog box next to the SQL definition.

3 DEM orchestrator and workers
   Upgrade all DEM orchestrators and workers. Finish the upgrade on one server before you upgrade the next server.
4 Agents

Finish the upgrade on one server before you upgrade the next server that is running an agent.

5 Management Agent

Is updated automatically as part of the upgrade process.

If you are using different services on one server, the upgrade updates the services in the proper order. For example, if your site has Web site and manager services on the same server, select both for update. The upgrade installer applies the updates in the proper order. You must complete the upgrade on one server before you begin an upgrade on another.

**Note** If your deployment uses a load balancer, the primary appliance must be connected to the load balancer. All other instances of vRealize Automation appliance appliances must be disabled for load balancer traffic before you apply the upgrade to avoid caching errors.

**Prerequisites**

- Back up your existing vRealize Automation environment.
- If you reboot an IaaS server after you update all the vRealize Automation appliances but before you upgrade the IaaS components, stop all of the IaaS windows services, except for the Management Agent service, on the server.
- **Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance.**
- Verify that your primary IaaS Website, Microsoft SQL database, and Model Manager node has JAVA SE Runtime Environment 8, 64bits, update 111 or later installed. After you install Java, you must set the environment variable, JAVA_HOME, to the new version on each server node.
- Verify that the creation date is earlier than the modified date in the web.config file. If the creation date for the web.config file is the same as or later than the modified date, perform the procedure in Upgrade Fails for IaaS Website Component.
- Complete these steps to reconfigure the Microsoft Distributed Transaction Coordinator (DTC).

**Note** Even with Distributed Transaction Coordinator enabled, the distributed transaction might fail if the firewall is turned on.

a On the vRealize Automation appliance, select **Start > Administrative Tools > Component Services**.

b Expand **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

c Choose the appropriate task.

- For a local standalone DTC, right-click **Local DTC** and select **Properties**
- For a clustered DTC expand **Clustered DTCs** and right-click the named clustered DTC and select **Properties**.
d  Click Security.

e  Select all of the following.
   - Network DTC Access
   - Allow Remote Clients
   - Allow Inbound
   - Allow Outbound
   - Mutual Authentication Required

f  Click OK.

Procedure

1  If you are using a load balancer, prepare your environment.
   a  Verify the IaaS Website node that contains the Model Manager data is enabled for load balancer traffic.
      You can identify this node by the presence of the vCAC Folder\Server\ConfigTool folder.
   b  Disable all other IaaS Websites and non-primary Manager Services for load balancer traffic.

2  Right-click the setup__vrealize-automation-appliance-FQDN@5480.exe setup file and select Run as administrator.

3  Click Next.

4  Accept the license agreement and click Next.

5  Type the administrator credentials for your current deployment on the Log In page.
   The user name is root and the password is the password that you specified when you deployed the appliance.

6  Select Accept Certificate.

7  On the Installation Type page, verify that Upgrade is selected.
   If Upgrade is not selected, the components on this system are already upgraded to this version.

8  Click Next.
9 Configure the upgrade settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are upgrading the Model Manager Data</td>
<td>Select the <strong>Model Manager Data</strong> check box in the vCAC Server section. The check box is selected by default. Upgrade the Model Manager data only once. If you are running the setup file on multiple machines to upgrade a distributed installation, the Web servers stop functioning while there is a version mismatch between the Web servers and the Model Manager data. When you have upgraded the Model Manager data and all of the Web servers, all of the Web servers should function.</td>
</tr>
<tr>
<td>If you are not upgrading the Model Manager Data</td>
<td>Unselect the <strong>Model Manager Data</strong> check box in the vCAC Server section.</td>
</tr>
<tr>
<td>To preserve customized workflows as the latest version in your Model Manager Data</td>
<td>If you are upgrading the Model Manager Data, select the <strong>Preserve my latest workflow versions</strong> check box in the Extensibility Workflows section. The check box is selected by default. Customized workflows are always preserved. The checkbox determines version order only. If you used vRealize Automation Designer to customize workflows in the Model Manager, select this option to maintain the most recent version of each customized workflow before upgrade as the most recent version after upgrade. If you do not select this option, the version of each workflow provided with vRealize Automation Designer becomes the most recent after upgrade, and the most recent version before upgrade becomes the second most recent. For information about vRealize Automation Designer, see <em>Extending Machine Life Cycles By Using vRealize Automation Designer</em>.</td>
</tr>
<tr>
<td>If you are upgrading a Distributed Execution Manager or a proxy agent</td>
<td>Enter the credentials for the administrator account in the Service Account section. All of the services that you upgrade run under this account.</td>
</tr>
<tr>
<td>To specify your Microsoft SQL Server database</td>
<td>If you are upgrading the Model Manager Data, enter the names of the database server and database instance in the <strong>Server</strong> text box in the Microsoft SQL Server Database Installation Information section. Enter a fully qualified domain name (FQDN) for the database server name in the <strong>Database name</strong> text box. If the database instance is on a non-default SQL port, include the port number in the server instance specification. The Microsoft SQL default port number is 1433. When upgrading the manager nodes, the MSSQL SSL option is selected by default. If your database does not use SSL, uncheck <strong>Use SSL for database connection</strong>.</td>
</tr>
</tbody>
</table>

10 Click **Next**.

11 Confirm that all services to upgrade appear on the Ready to Upgrade page, and click **Upgrade**.

The Upgrading page and a progress indicator appear. When the upgrade process finishes, the **Next** button is enabled.

12 Click **Next**.

13 Click **Finish**.

14 Verify that all services restarted.

15 Repeat these steps for each IaaS server in your deployment in the recommended order.
After all components are upgraded, log in to the management console for the appliance and verify that all services, including IaaS, are now registered.

(Optional) Enable Automatic Manager Service Failover. See Enable Automatic Manager Service Failover After Upgrade.

All of the selected components are upgraded to the new release.

What to do next

1. Restore Access to the Built-In vRealize Orchestrator Control Center.
2. If your deployment uses a load balancer, upgrade each load balancer node to use vRealize Automation health checks, and re-enable load balancer traffic for any unconnected nodes.
   For more information, see vRealize Automation Load Balancing.

Restore Access to the Built-In vRealize Orchestrator Control Center

After you upgrade the IaaS server components, you must restore access to vRealize Orchestrator.

When you upgrade from vRealize Automation 7.3 and earlier to 7.4, you need to perform this procedure to accommodate the new Role-Based Access Control feature. This procedure is written for a high-availability environment.

Prerequisites

Make a snapshot of your vRealize Automation environment.

Procedure

1. Log in to the vRealize Automation appliance management console as root by using the appliance host fully qualified domain name, https://va-hostname.domain.name:5480.
2. Select vRA Settings > Database.
3. Identify the master and replica nodes.
4. On each replica node, open an SSH session, log in as administrator, and run this command:
   
   ```
   service vco-server stop && service vco-configurator stop
   ```
5. On the master node, open an SSH session, log in as administrator, and run this command:
   
   ```
   rm /etc/vco/app-server/vco-registration-id
   ```
6. On the master node, change directories to /etc/vco/app-server/.
7. Open the sso.properties file.
If the property name `com.vmware.o11n.sso.admin.group.name` contains spaces or any other Bash-related characters that can be accepted as a special character in a Bash command such as a hyphen (') or a dollar sign ($), complete these steps.

a. Copy the line with the `com.vmware.o11n.sso.admin.group.name` property and enter `AdminGroup` for the value.

b. Add `#` to the beginning of the original line with the `com.vmware.o11n.sso.admin.group.name` property to comment the line.

c. Save and close the `sso.properties` file.

Run this command:
```
vcac-vami vco-service-reconfigure
```

Open the `sso.properties` file. If the file has changed, complete these steps.

a. Remove the `#` from the beginning of the original line with the `com.vmware.o11n.sso.admin.group.name` property to uncomment the line.

b. Remove the copy of the line with the `com.vmware.o11n.sso.admin.group.name` property.

c. Save and close the `sso.properties` file.

Run this command to restart the `vco-server` service:
```
service vco-server restart
```

Run this command to restart the `vco-configurator` service:
```
service vco-configurator restart
```

In the vRealize Automation appliance management console, click `Services` and wait until all the services in the master node are REGISTERED.

When all the services are registered, join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the vRealize Orchestrator configuration. For information, see Reconfigure the Built-In vRealize Orchestrator to Support High Availability.

What to do next

Upgrading vRealize Orchestrator After Upgrading vRealize Automation.

Upgrading vRealize Orchestrator After Upgrading vRealize Automation

You must upgrade your vRealize Orchestrator instance when you upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4.

With the release of vRealize Orchestrator 7.4, you have two options for upgrading vRealize Orchestrator when you upgrade to vRealize Automation 7.4.

- You can migrate your existing external vRealize Orchestrator server to the embedded vRealize Orchestrator included in vRealize Automation 7.4.

- You can upgrade your existing standalone or clustered vRealize Orchestrator server to work with vRealize Automation 7.4.
Migrating an External vRealize Orchestrator Server to vRealize Automation

You can migrate your existing external vRealize Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

You can deploy vRealize Orchestrator as an external server instance and configure vRealize Automation to work with that external instance, or you can configure and use the vRealize Orchestrator server that is included in the vRealize Automation appliance.

VMware recommends that you migrate your external vRealize Orchestrator to the Orchestrator server that is built into vRealize Automation. The migration from an external to embedded Orchestrator provides the following benefits:

- Reduces the total cost of ownership.
- Simplifies the deployment model.
- Improves the operational efficiency.

Note Consider using the external vRealize Orchestrator in the following cases:

- Multiple tenants in the vRealize Automation environment
- Geographically dispersed environment
- Workload handling
- Use of specific plug-ins, such as older versions of the Site Recovery Manager plug-in

Control Center Differences Between External and Embedded Orchestrator

Some of the menu items that are available in Control Center of an external vRealize Orchestrator are not included in the default Control Center view of an embedded Orchestrator instance.

In Control Center of the embedded Orchestrator server, a few options are hidden by default.

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.</td>
</tr>
<tr>
<td>Export/Import Configuration</td>
<td>The embedded Orchestrator configuration is included in the exported vRealize Automation components.</td>
</tr>
<tr>
<td>Configure Database</td>
<td>The embedded Orchestrator uses the database that is used by vRealize Automation.</td>
</tr>
<tr>
<td>Customer Experience Improvement Program</td>
<td>You can join the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance management interface.</td>
</tr>
<tr>
<td></td>
<td>See The Customer Experience Improvement Program in Managing vRealize Automation.</td>
</tr>
</tbody>
</table>

Another options that are hidden from the default Control Center view are the **Host address** text box and the **UNREGISTER** button on the **Configure Authentication Provider** page.

Note To see the full set of Control Center options in vRealize Orchestrator that is built into vRealize Automation, you must access the advanced Orchestrator Management page at https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter#/?advanced and click the F5 button on the keyboard to refresh the page.
Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4

You can export the configuration from your existing external Orchestrator instance and import it to the Orchestrator server that is built into vRealize Automation.

**Note** If you have multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see *Upgrading vRealize Automation* in *Installing or Upgrading vRealize Automation*.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

**Procedure**

1. Export the configuration from the external Orchestrator server.
   - Log in to Control Center of the external Orchestrator server as **root** or as an **administrator**, depending on the source version.
   - Stop the Orchestrator server service from the **Startup Options** page to prevent unwanted changes to the database.
   - Go to the **Export/Import Configuration** page.
   - On the **Export Configuration** page, select **Export server configuration**, **Bundle plug-ins** and **Export plug-in configurations**.

2. Migrate the exported configuration into the embedded Orchestrator instance.
   - Upload the exported Orchestrator configuration file to the `/usr/lib/vco/tools/configuration-cli/bin` directory of the vRealize Automation appliance.
   - Log in to the vRealize Automation appliance over SSH as **root**.
   - Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

   ```bash
   service vco-server stop && service vco-configurator stop
   ```

   - Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

   ```bash
   ./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
   ```
3 If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.
   a In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.
   b Set the values of `listen_addresses` to a wildcard (`*`).
      ```
      listen_addresses = '*'
      ```
   c Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.
      ```
      host all all vra-va-ip-address/32 md5
      ```
      **Note** The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.
   d Restart the PostgreSQL server service.
      ```
      service vpostgres restart
      ```

4 Migrate the database to the internal PostgreSQL database, by running the `vro-configure` script with the `db-migrate` command.
   ```
   ./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
   ```
   **Note** Enclose passwords that contain special characters in single quotation marks.

The `JDBC_connection_URL` depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th>Database Name</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_name</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>
5 Remove all certificates from the database keystore.

   ./vro-configuration.sh untrust --reset-db

6 Reinstall the Orchestrator plug-ins.
   a Log in to Control Center as root.
   b Click Troubleshooting.
   c Click Force plug-ins reinstall.

7 Start the Orchestrator server service.

8 Revert to the default configuration of the postgresql.conf and the pg_hba.conf file.
   a Restart the PostgreSQL server service.

You successfully migrated an external Orchestrator server instance to a vRealize Orchestrator instance embedded in vRealize Automation.

What to do next
Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

Configure the Built-In vRealize Orchestrator Server

After you export the configuration of an external Orchestrator server and import it to vRealize Automation 7.4, you must configure the Orchestrator server that is built into vRealize Automation.

Prerequisites

Migrate the configuration from the external to the internal vRealize Orchestrator.

Procedure

1 Log in to the vRealize Automation appliance over SSH as root.

2 Start the Control Center service and the Orchestrator server service of the built-in vRealize Orchestrator server.

   service vco-configurator start & service vco-server start

3 Log in to Control Center of the built-in Orchestrator server as an administrator.

   Note If you migrate from an external vRealize Orchestrator 7.4 instance, skip to step 5.

4 Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.
If the external Orchestrator was configured to work in cluster mode, reconfigure the Orchestrator cluster in vRealize Automation.

a Go to the advanced Orchestrator Cluster Management page, at https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/control-app/ha?remove-nodes.

Note If the Remove check boxes next the existing nodes in the cluster do not appear, you must refresh the browser page by clicking the F5 button on the keyboard.

b Select the check boxes next to the external Orchestrator nodes and click Remove to remove them from the cluster.

c To exit the advanced cluster management page, delete the remove-nodes string from the URL and refresh the browser page by clicking the F5 button on the keyboard.

d At the Validate Configuration page in Control Center, verify that Orchestrator is configured properly.

6 (Optional) Under the Package Signing Certificate tab on the Certificates page, generate a new package signing certificate.

7 (Optional) Change the values for Default tenant and Admin group on the Configure Authentication Provider page.

8 Verify that the vco-server service appears as REGISTERED under the Services tab in the vRealize Automation appliance management console.

9 Select the vco services of the external Orchestrator server and click Unregister.

What to do next

- Import any certificates that were trusted in the external Orchestrator server to the trust store of the built-in Orchestrator.
- Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the Orchestrator configuration.

For more information, see Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability in Installing or Upgrading vRealize Automation.

Note The vRealize Orchestrator instances are automatically clustered and available for use.

- Restart the vco-configurator service on all nodes in the cluster.
- Update the vRealize Orchestrator endpoint to point to the migrated built-in Orchestrator server.
- Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.
Upgrading a Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation

If you maintain a stand-alone, external instance of vRealize Orchestrator for use with vRealize Automation, you must upgrade vRealize Orchestrator when you upgrade vRealize Automation from 7.1, 7.2, or 7.3.x to 7.4.

Embedded instances of vRealize Orchestrator are upgraded as part of the vRealize Automation appliance upgrade. No additional action is required for an embedded instance.

If you are upgrading a vRealize Orchestrator appliance cluster, see Upgrade a vRealize Orchestrator Appliance Cluster for Use with vRealize Automation 7.4.

Prerequisites

- Install the Update on the vRealize Automation Appliance and IaaS Components.
- Unmount all network file systems. See vSphere Virtual Machine Administration in the vSphere documentation.
- Increase the memory of the vSphere Orchestrator appliance to at least 6 GB. See vSphere Virtual Machine Administration in the vSphere documentation.
- Take a snapshot of the vSphere Orchestrator virtual machine. See vSphere Virtual Machine Administration in the vSphere documentation.
- If you use an external database, back up the database.
- If you use the preconfigured PostgreSQL database in vSphere Orchestrator, back up the database by using the Export Database menu in the vSphere Control Center.

Procedure

- Use one of the documented methods to upgrade your stand-alone vRealize Orchestrator.
  - Upgrade Orchestrator Appliance by Using the Default VMware Repository.
  - Upgrade Orchestrator Appliance by Using an ISO Image.
  - Upgrade Orchestrator Appliance by Using a Specified Repository.

Upgrade Orchestrator Appliance by Using the Default VMware Repository

You can configure Orchestrator to download the upgrade package from the default VMware repository.

Prerequisites

- Unmount all network file systems. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
- Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.
Take a snapshot of the Orchestrator virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.

- If you use an external database, back up the database.
- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

**Procedure**

1. Go to the Virtual Appliance Management Interface (VAMI) at https://orchestrator_server:5480 and log in as **root**.
2. On the **Update** tab, click **Settings**.
   The radio button next to the **Use Default Repository** option is selected.
3. On the **Status** page, click **Check Updates**.
4. If any updates are available, click **Install Updates**.
5. Accept the VMware End-User License Agreement and confirm that you want to install the update.
6. To complete the update, restart the Orchestrator Appliance.
   a. Log in again to the Virtual Appliance Management Interface (VAMI) as **root**.
7. (Optional) On the **Update** tab, verify that the latest version of the Orchestrator Appliance is successfully installed.
8. Log in to Control Center as **root**.
9. If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.
   a. On the **Host Settings** page in Control Center, click **CHANGE**.
   b. Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.
10. Reconfigure the authentication.
    a. If before the upgrade, the Orchestrator server was configured to use **LDAP** or **SSO (legacy)** as an authentication method, configure **vSphere** or **vRealize Automation** as an authentication provider.
    b. If the authentication is already set to **vSphere** or **vRealize Automation**, unregister the settings and register them again.

**Note** If before the upgrade, your Orchestrator used **vSphere** as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.
You successfully upgraded the Orchestrator Appliance.

What to do next

Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

Upgrade Orchestrator Appliance by Using an ISO Image

You can configure Orchestrator to download the upgrade package from an ISO image file mounted to the CD-ROM drive of the appliance.

Prerequisites

- Unmount all network file systems. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
- Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.
- Take a snapshot of the Orchestrator virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.
- If you use an external database, back up the database.
- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

Procedure

1. Download the VMware-vRO-Appliance-version-build_number-updaterepo.iso archive from the official VMware download site.
2. Connect the CD-ROM drive of the Orchestrator Appliance virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.
3. Mount the ISO image file to the CD-ROM drive of the appliance. For more information, see the vSphere Virtual Machine Administration documentation.
5. On the Update tab, click Settings.
6. Select the radio button next to the Use CD-ROM updates option.
7. Return to the Status page.
   - The version of the available upgrade is displayed.
8. Click Install Updates.
9 Accept the VMware End-User License Agreement and confirm that you want to install the update.

10 To complete the update, restart the Orchestrator Appliance.
   a Log in again to the Virtual Appliance Management Interface (VAMI) as root.

11 (Optional) On the Update tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

12 Log in to Control Center as root.

13 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.
   a On the Host Settings page in Control Center, click CHANGE.
   b Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

14 Reconfigure the authentication.
   a If before the upgrade, the Orchestrator server was configured to use LDAP or SSO (legacy) as an authentication method, configure vSphere or vRealize Automation as an authentication provider.
   b If the authentication is already set to vSphere or vRealize Automation, unregister the settings and register them again.

   **Note** If before the upgrade, your Orchestrator used vSphere as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.

You successfully upgraded the Orchestrator Appliance.

**What to do next**

Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

**Upgrade Orchestrator Appliance by Using a Specified Repository**

You can configure Orchestrator to use a local repository, on which you uploaded the upgrade archive.

**Prerequisites**

- Unmount all network file systems. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.

Take a snapshot of the Orchestrator virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.

If you use an external database, back up the database.

If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

Procedure

1. Prepare the local repository for upgrades.
   a. Install and configure a local Web server.
   b. Download the VMware-vRO-Appliance-version-build_number-updaterrepo.zip archive from the official VMware download site.
   c. Extract the .ZIP archive to the local repository.

2. Go to the Virtual Appliance Management Interface (VAMI) at https://orchestrator_server:5480 and log in as root.

3. On the Update tab, click Settings.

4. Select the radio button next to the Use Specified Repository option.

5. Enter the URL address of the local repository by pointing to the Update_Repo directory.

6. If the local repository requires authentication, enter user name and password.

7. Click Save Settings.

8. On the Status page, click Check Updates.

9. If any updates are available, click Install Updates.

10. Accept the VMware End-User License Agreement and confirm that you want to install the update.

11. To complete the update, restart the Orchestrator Appliance.
   a. Log in again to the Virtual Appliance Management Interface (VAMI) as root.

12. (Optional) On the Update tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

13. Log in to Control Center as root.
14 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.
   a On the Host Settings page in Control Center, click CHANGE.
   b Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

15 Reconfigure the authentication.
   a If before the upgrade, the Orchestrator server was configured to use LDAP or SSO (legacy) as an authentication method, configure vSphere or vRealize Automation as an authentication provider.
   b If the authentication is already set to vSphere or vRealize Automation, unregister the settings and register them again.

   **Note** If before the upgrade, your Orchestrator used vSphere as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.

You successfully upgraded the Orchestrator Appliance.

**What to do next**

Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

**Upgrade a vRealize Orchestrator Appliance Cluster for Use with vRealize Automation 7.4**

If you use a vRealize Orchestrator appliance cluster with vRealize Automation, you must upgrade the Orchestrator appliance cluster to version 7.4 by upgrading a single instance and joining newly installed 7.4 nodes to the upgraded instance.

To upgrade a single instance of vRealize Orchestrator, see Upgrading a Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation.

**Prerequisites**

- Install the Update on the vRealize Automation Appliance and IaaS Components.
- Set up a load balancer to distribute traffic among multiple instances of vRealize Orchestrator. See the vRealize Orchestrator Load Balancing Configuration Guide.
- Take a snapshot of all vRealize Orchestrator server nodes.
- Back up the vRealize Orchestrator shared database.

**Procedure**

1 Stop the vco-server and vco-configurator Orchestrator services on all cluster nodes.
Upgrade only one of the Orchestrator server instances in your cluster using one of the documented procedures.

Deploy a new Orchestrator appliance on version 7.3.

- Configure the new node with the network settings of an existing not upgraded instance that is part of the cluster.

Access Control Center of the second node to start the configuration wizard.

- Navigate to https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter.
- Log in as root with the password you entered during OVA deployment.

Select the Clustered Orchestrator deployment type.

By choosing this type, you select to join the node to an existing Orchestrator cluster.

In the Hostname text box, enter the host name or IP address of the first Orchestrator server instance.

**Note** This must be the local IP or host name of the Orchestrator instance, to which you are joining the second node. You must not use the load balancer address.

In the User name and Password text boxes, enter the root credentials of the first Orchestrator server instance.

Click Join. The Orchestrator instance clones the configuration of the node, to which it joins.

The Orchestrator server service of both nodes restart automatically.

Access Control Center of the upgraded Orchestrator cluster through the load balancer address and log in as an administrator.

On the Orchestrator Cluster Management page, make sure that the Active Configuration Fingerprint and the Pending Configuration Fingerprint strings on all nodes in the cluster match.

**Note** You might need to refresh the page several times until the two strings match.

Verify that the vRealize Orchestrator cluster is configured properly by opening the Validate Configuration page in Control Center.

(Optional) Repeat steps 3 through 8 for each additional node in the cluster.

You have successfully upgraded the Orchestrator cluster.

**What to do next**

Enable Your Load Balancers.

**Migrating to vRealize Automation 7.4**

You can perform a side-by-side upgrade of your current vRealize Automation environment to the latest version using migration.

This information is specific to upgrading vRealize Automation to 7.4 using migration. For information about other supported upgrade paths, see Upgrading vRealize Automation.
Migrating vRealize Automation

You can perform a side-by-side upgrade of your current vRealize Automation environment using migration.

Migration moves all data, except for tenants and identity stores, from your current vRealize Automation source environment to a target deployment of the latest version of vRealize Automation. In addition, migration moves all data from the embedded vRealize Orchestrator 7.x to the target deployment.

Migration does not change your source environment except to stop vRealize Automation services for the time required to collect and copy the data safely to your target environment. Depending on the size of the source vRealize Automation database, migration can take from a few minutes to hours.

You can migrate your source environment to a minimal deployment or a high-availability deployment.

If you plan to put your target environment into production after migration, do not put your source environment back into service. Changes to your source environment after migration are not synchronized with your target environment.

If your source environment is integrated with vCloud Air or vCloud Director or has physical endpoints, you must use migration to perform an upgrade. Migration removes these endpoints and everything associated with them from the target environment. Migration also removes a 6.x VMware vRealize Application Services integration from the target environment.

**Note**  You must complete additional tasks to prepare your vRealize Automation virtual machines before you migrate. Before you migrate, review Knowledge Base article 51531.

If you migrate from vRealize Automation 6.2.x to the latest version, you might experience these issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request.</td>
<td>You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request.</td>
</tr>
<tr>
<td>Control types: Check box or link.</td>
<td></td>
</tr>
<tr>
<td>Attributes: Relationship, regular expressions, or property layouts.</td>
<td></td>
</tr>
<tr>
<td>In vRealize Automation 7.x, the property definitions no longer use these elements.</td>
<td></td>
</tr>
<tr>
<td>Regular expressions used to define the parent-child relationships in a vRealize Automation 6.2.x drop-down menu are not supported in 7.x. In 6.2.x, you can use regular expressions to define one or more child menu items that are only available for a certain parent menu item. Only those child menu items appear when you select the parent menu item. After migration to 7.x, all the available menu items appear in the child drop-down menu regardless of what you choose in the parent drop-down menu. To show that previously defined dynamic values no longer work, the first menu item in the child drop-down menu reads &quot;Warning! Use vRO workflows to define dynamic values.&quot;</td>
<td>After migration, you must recreate the property definition to restore the previous dynamic values. For information about creating a parent-child relationship between the parent drop-down menu and the child drop-down menu, see How to use dynamic property definitions in vRA 7.2.</td>
</tr>
</tbody>
</table>
vRealize Automation Environment User Interfaces

You use and manage your vRealize Automation environment with several interfaces.

User Interfaces

These tables describe the interfaces that you use to manage your vRealize Automation environment.

Table 1-56. vRealize Automation Administration Console

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the vRealize Automation console for these system administrator tasks. | 1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.  
| Add tenants. | 2 Click vRealize Automation console. | You must be a user with the system administrator role.  
| Customize the vRealize Automation user interface. |  
| Configure email servers. | You can also use this URL to open the vRealize Automation console: https://vra-va-hostname.domain.name/vcac. |  
| View event logs. | 3 Log in. |  
| Configure vRealize Orchestrator. | | |

Table 1-57. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use vRealize Automation for these tasks. | 1 Start a browser and enter the URL of your tenancy using the fully qualified domain name of the virtual appliance and the tenant URL name: https://vra-va-hostname.domain.name/vcac/tenant_URL_name. | You must be a user with one or more of these roles:  
| Request new IT service blueprints. | 2 Log in. | Application Architect  
| Create and manage cloud and IT resources. |  
| Create and manage custom groups. | Approval Administrator  
| Create and manage business groups. | Catalog Administrator  
| Assign roles to users. | Container Administrator  
| | Container Architect  
| | Health Consumer  
| | Infrastructure Architect  
| | Secure Export Consumer  
| | Software Architect  
| | Tenant Administrator  
| | XaaS Architect |
Table 1-58. vRealize Automation Appliance Management. This interface is sometimes called the Virtual Appliance Management Interface (VAMI).

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use vRealize Automation Appliance Management for these tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>User name: root</td>
</tr>
<tr>
<td></td>
<td>2 Click vRealize Automation Appliance Management. You can also use this URL to open vRealize Automation Appliance Management: <a href="https://vra-va-hostname.domain.name:5480">https://vra-va-hostname.domain.name:5480</a>.</td>
<td>Password: Password you entered when you deployed the vRealize Automation appliance.</td>
</tr>
<tr>
<td></td>
<td>3 Log in.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-59. vRealize Orchestrator Client

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Orchestrator Client for these tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>You must be a user with the system administrator role or part of the vcoadmins group configured in the vRealize Orchestrator Control Center Authentication Provider settings.</td>
</tr>
<tr>
<td></td>
<td>2 To download the client.jnlp file to your local computer, click vRealize Orchestrator Client.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Right-click the client.jnlp file and select Launch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 On the Do you want to Continue? dialog box, click Continue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Log in.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-60. vRealize Orchestrator Control Center

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the vRealize Orchestrator Control Center to edit the configuration of the default vRealize Orchestrator instance that is embedded in vRealize Automation. | 1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.  
2 Click vRealize Automation Appliance Management.  
You can also use this URL to open vRealize Automation Appliance Management: https://vra-va-hostname.domain.name:5480.  
3 Log in.  
4 Click vRA Settings > Orchestrator.  
5 Select Orchestrator user interface.  
6 Click Start.  
7 Click the Orchestrator user interface URL.  
8 Log in. | User Name  
- Enter root if role-based authentication is not configured.  
- Enter your vRealize Automation user name if it is configured for role-based authentication.  
Password  
- Enter the password you entered when you deployed the vRealize Automation appliance if role-based authentication is not configured.  
- Enter the password for your user name if your user name is configured for role-based authentication. |

### Table 1-61. Linux Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the Linux command prompt on a host, such as the vRealize Automation appliance host, for these tasks.  
- Stop or start services  
- Edit configuration files  
- Run commands  
- Retrieve data | 1 On the vRealize Automation appliance host, open a command prompt.  
One way to open the command prompt on your local computer is to start a session on the host using an application such as PuTTY.  
2 Log in. | User name: root  
Password: Password you created when you deployed the vRealize Automation appliance. |

### Table 1-62. Windows Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You can use a Windows command prompt on a host, such as the IaaS host, to run scripts. | 1 On the IaaS host, log in to Windows.  
One way to log in from your local computer is to start a remote desktop session.  
2 Open the Windows command prompt.  
One way to open the command prompt is to right-click the Start icon on the host and select Command Prompt or Command Prompt (Admin). | User name: User with administrative privileges.  
Password: User's password. |
Migration Prerequisites
The migration prerequisites differ depending on your target environment.

You can migrate to a minimal environment or to a high-availability environment.

Prerequisites for Migration to a Minimal Environment

Ensure a successful migration to a minimal environment by reviewing these prerequisites.

Minimal deployments include one vRealize Automation appliance and one Windows server that hosts the IaaS components. In a minimal deployment, the vRealize Automation SQL Server database can be on the same IaaS Windows server with the IaaS components, or on a separate Windows server.
Figure 1-17. vRealize Automation Minimal Deployment

vRealize Automation Appliance

vRealize Orchestrator

PostgreSQL DB

vRealize Automation Infrastructure as a service (IaaS)

Microsoft IIS

IaaS Web

Model Manager Repository

Manager Service

DEM Orchestrator

DEM Worker

Proxy Agent

Microsoft SQL Server DB
Prerequisites

- Verify that you have a new target environment of vRealize Automation.
- Install relevant proxy agents on the target environment according to these requirements.
  - Target proxy agent name must match the source proxy agent name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.

  **Note** Finish these steps to obtain an agent name.

  1. On the IaaS host, log in to Windows as a local user with administrator privileges.
  2. Use Windows Explorer to go to the agent installation directory.
  3. Open the `VRMAgent.exe.config` file.
  4. Under the `serviceConfiguration` tag, look for the value of the `agentName` attribute.

- Review Knowledge Base article 51531.
- Target proxy agent endpoint name must match the source proxy agent endpoint name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.
- Do not create an endpoint for vSphere, Hyper-V, Citrix XenServer, or Test proxy agents on the target environment.
- Review the version numbers of vRealize Automation components on the target vRealize Automation appliance.
  a. Log in to the target vRealize Automation Appliance Management as root using the password you entered when you deployed the target vRealize Automation appliance.
  b. Select **vRA Settings > Cluster**.
  c. Expand the Host / Node Name records by clicking the triangle.

  Verify that the version numbers of the vRealize Automation IaaS components match.
- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.
- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.
- Verify that the endpoint vCenter has sufficient resources to complete migration.
- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.
- Verify that the IaaS server node in the target environment has at least Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. After you install the JRE, make sure the `JAVA_HOME` environment variable points to the Java version you installed on each IaaS node. Revise the path if necessary.
- Verify that each IaaS node has PowerShell 3.0 or later installed.
- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.
- Verify that the IaaS Web Service and Model Manager do not need to be restarted because of pending Windows installation updates. Pending updates might prevent the migration to begin or end the World Wide Web Publishing Service.

What to do next

Pre-Migration Tasks.

Prerequisites for Migration to a High-Availability Environment

Ensure a successful migration to a high-availability environment by reviewing these prerequisites.

High-availability environments can be of varying size. A basic distributed deployment might improve vRealize Automation simply by hosting IaaS components on separate Windows servers. Many high-availability environments go even further, with redundant appliances, redundant servers, and load balancing for even more capacity. Large, distributed deployments provide for better scale, high availability, and disaster recovery.
Figure 1-18. vRealize Automation High-Availability Environment
Prerequisites

- Verify that you have a new target installation of vRealize Automation with a master and replica virtual appliance configured for high availability. See vRealize Automation High Availability Configuration Considerations.
- Verify that all vRealize Automation virtual appliances use the same password for root user.
- Install relevant proxy agents on the target environment according to these requirements.
  - Target proxy agent name must match the source proxy agent name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.

  **Note** Finish these steps to obtain an agent name.

  1. On the IaaS host, log in to Windows as a local user with administrator privileges.
  2. Use Windows Explorer to go to the agent installation directory.
  3. Open the VRMAgent.exe.config file.
  4. Under the serviceConfiguration tag, look for the value of the agentName attribute.

- Target proxy agent endpoint name must match the source proxy agent endpoint name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.
- Do not create an endpoint for vSphere, Hyper-V, Citrix XenServer, or Test proxy agents on the target environment.
- Check the version numbers of vRealize Automation components on the target vRealize Automation appliance.
  b. Log in with the user name root and the password you entered when you deployed the appliance.
  c. Select vRA Settings > Cluster.
  d. To expand the Host / Node Name records so you can see the components, click the expand button.
    - Verify that the version numbers of vRealize Automation components match across all virtual appliance nodes.
    - Verify that the version numbers of vRealize Automation IaaS components match across all IaaS nodes.
- Review Knowledge Base article 51531.
- Perform these steps to direct traffic to only the master node.
  a. Disable all the redundant nodes.
b Remove the health monitors for these items according to your load balancer documentation:

- vRealize Automation virtual appliance
- IaaS Website
- IaaS Manager Service

- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.
- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.
- Verify that the endpoint vCenter has sufficient resources to complete migration.
- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.
- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.
- Verify that the IaaS Web Service and Model Manager nodes in the target environment have the right Java Runtime Environment. You must have Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. Make sure the JAVA_HOME system variable points to the Java version you installed on each IaaS node. Revise the path if necessary.
- Verify that each IaaS node has at least PowerShell 3.0 or later installed.
- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.
- Verify that the IaaS Web Service and Model Manager do not need to be restarted because of pending Windows installation updates. Pending updates might prevent the migration to begin or end the World Wide Web Publishing Service.

What to do next

Pre-Migration Tasks.

Pre-Migration Tasks

Before you migrate, you must perform several pre-migration tasks.

The pre-migration tasks you perform before you migrate your source vRealize Automation environment data to the target vRealize Automation environment vary depending on your source environment.

Review Changes Introduced by Migration from vRealize Automation 6.2.x to 7.x

vRealize Automation 7 and later introduces various functional changes during and after the upgrade process. Review these changes before you upgrade your vRealize Automation 6.2.x deployment to the latest version.
For information about the differences between vRealize Automation 6.2.x and 7.x, see Considerations About Upgrading to This vRealize Automation Version in Upgrading vRealize Automation 6.2.5 to 7.4.

**Note** The vRealize Production Test Upgrade Assist Tool analyzes your vRealize Automation 6.2.x environment for any feature configuration that can cause upgrade issues and checks that your environment is ready for upgrade. To download this tool and related documentation, go to the VMware vRealize Production Test Tool download product page.

After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request.

- Control types: Check box or link.
- Attributes: Relationship, regular expressions, or property layouts.

In vRealize Automation 7.x, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request.

**Apply Software Agent Patch**

Before you migrate from vRealize Automation 7.1 or 7.3 to 7.4, you must apply a hot fix to the source appliance so that you can upgrade Software Agents to TLS 1.2.

The Transport Layer Security (TLS) protocol provides data integrity between your browser and vRealize Automation. This hot fix makes it possible for the Software Agents in your source environment to upgrade to TLS 1.2. This upgrade ensures the highest level of security and is required for vRealize Automation 7.1 or 7.3. Each version has its own hot fix.

**Prerequisites**

A running vRealize Automation 7.1 or 7.3 source environment.

**Procedure**

- Apply this hot fix to your source vRealize Automation 7.1 or 7.3 appliance before you migrate to 7.4. See Knowledge Base article 52897.

**What to do next**

**Change DoDeletes Setting on the vSphere Agent to False.**

If you migrate from a vRealize Automation 6.2.x environment, you must change the DoDeletes value from **true** to **false** on your target vSphere agent before migration.

**Prerequisites**

Finish the prerequisites for migration.
Procedure

1. Change the DoDeletes value to **false**.

   This prevents deletion of your virtual machines from the source environment. The source and target environments run in parallel. Lease discrepancies might arise after the production migration is validated.

2. Set the DoDeletes value to **true** after your production migration is validated and your source environment shuts down.

3. Follow the steps in the **Configure the vSphere Agent** procedure to set DoDeletes to **false**.

What to do next

**Prepare vRealize Automation Virtual Machines for Migration.**

Check Templates in Your vRealize Automation Source Environment

Before you migrate vRealize Automation, you must check your virtual machine templates to make sure that every template has a minimum memory setting of at least 4 MB.

If you have a virtual machine template in your vRealize Automation source environment with less than 4 MB of memory, migration fails. Complete this procedure to determine if any blueprints in the source environment have less than 4 MB of memory.

Prerequisites

Procedure

1. Log in to the windows server hosting your SQL server database.

2. Open the SQL Server Management Studio and connect to your vRA database.

3. Run this script to check if there are any blueprints with memory specified at less than 4 MB.

   ```
   select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and MemoryMB < 4;
   ```

   where vCAC is the database name.

4. If the script finds any blueprints with memory specified at less than 4 MB, then run this script to update the memory to at least 4 MB.

   ```
   update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
   ```

   where vCAC is the database name.

What to do next

**Prepare vRealize Automation Virtual Machines for Migration.**
You must review Knowledge Base article 000051531 and perform any relevant fixes to your environments prior to migration.

What to do next

Gather Information Required for Migration.

Use these tables to record the information that you need for migration from your source and target environments.

Prerequisites

Finish verifying the prerequisites for your situation.

- Prerequisites for Migration to a Minimal Environment.
- Prerequisites for Migration to a High-Availability Environment.

**Table 1-63. Source vRealize Automation Appliance**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Log in to your source vRealize Automation Appliance Management. Find the host name on the System tab. The host name must be a fully qualified domain name (FQDN).</td>
<td></td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed your source vRealize Automation appliance.</td>
<td></td>
</tr>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created. The directory must have available space that is twice as big as the size of the vRealize Automation database. The default location is /storage.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1-64. Target vRealize Automation Appliance**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed your target vRealize Automation appliance.</td>
<td></td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local</td>
<td></td>
</tr>
<tr>
<td>Administrator username</td>
<td>administrator</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-65. Target IaaS Database

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>Location of Microsoft SQL Server instance where the cloned database resides. If named instance and a non-default port is used, specify in SERVER,PORT\INSTANCE-NAME format.</td>
<td></td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation6.2.x/7.x IaaS Microsoft SQL database cloned for migration.</td>
<td></td>
</tr>
<tr>
<td>Authentication mode</td>
<td>Select either Windows or SQL Server. If you select SQL Server, you must enter a login name and password.</td>
<td></td>
</tr>
<tr>
<td>Login name</td>
<td>Login name for the SQL Server user who has the db_owner role for the cloned IaaS Microsoft SQL database.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SQL Server user.</td>
<td></td>
</tr>
<tr>
<td>Original encryption key</td>
<td>Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment.</td>
<td></td>
</tr>
<tr>
<td>New passphrase</td>
<td>A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment.</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

**Obtain the Encryption Key from the Source vRealize Automation Environment.**

You must enter the encryption key from the source vRealize Automation environment as part of the migration procedure.

**Prerequisites**

Verify that you have administrator privileges on the active Manager Service host virtual machine in your source environment.

**Procedure**

1. Open a command prompt as an administrator on the virtual machine that hosts the active Manager Service in your source environment and run this command.

   ```
   "C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config" -v
   ```

   If your installation directory is not in the default location, `C:\Program Files (x86)\VMware\vCAC`, edit the path to show your actual installation directory.
Save the key that appears after you run the command.
The key is a long string of characters that looks similar to this example:
NRH+f/B1nCB6yvasLS3sxspsgdkcFWAEuyV0g4lfryg=.

What to do next

- If you are migrating from a vRealize Automation 6.2.x environment: Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.

- If you are migrating from a vRealize Automation 7.x environment: List Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment.

List Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment

Before you migrate a vRealize Automation 6.2.x environment, you must make a list of the tenant and IaaS administrators for each tenant.

Perform the following procedure for each tenant in the source vRealize Automation console.

**Note** If you migrate from a vRealize Automation 7.x environment, you do not need to perform this procedure.

**Prerequisites**

Log in to the source vRealize Automation console as Administrator with the password you entered when you deployed the source vRealize Automation appliance.

**Note** For a high-availability environment, open the console using the fully qualified domain name of the source virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

**Procedure**

1. Select Administration > Tenants.
2. Click a tenant name.
3. Click Administrators.
4. Make a list of each tenant and IaaS administrator user name.
5. Click Cancel.

**What to do next**

Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.

Add Each Tenant from the Source vRealize Automation Environment to the Target Environment

You must add tenants in the target environment using the name of each tenant in the source environment.
For successful migration, it is mandatory that each tenant in the source environment is created in the target environment. You must also use a tenant-specific access URL for each tenant that you add using the tenant URL name from the source environment. If there are unused tenants in the source environment that you do not want to migrate, delete them from the source environment before migration.

**Note** Migration validation ensures that the target system has at least the same tenants configured in the source as required by the prerequisites. It performs tenant comparison based on case-sensitive tenant URL names, not the tenant names.

Perform this procedure for each tenant in your source environment.

- When you migrate from a vRealize Automation 6.2.x environment, you migrate your existing SSO2 tenants and identity stores on the source environment to the VMware Identity Manager on the target environment.
- When you migrate from a vRealize Automation 7.x environment, you migrate your existing VMware Identity Manager tenants and identity stores on the source environment to the VMware Identity Manager on the target environment.

**Prerequisites**

- **Gather Information Required for Migration.**
- Log in to the target vRealize Automation console as **Administrator** with the password you entered when you deployed the target vRealize Automation appliance.

  **Note** For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

**Procedure**

1. Select **Administration > Tenants**.
2. Click the **New** icon (➕).
3. In the **Name** text box, enter a tenant name that matches a tenant name in the source environment.
   
   For example, if the tenant name in the source environment is DEVTenant, enter **DEVTenant**.
4. (Optional) Enter a description in the **Description** text box.
5. In the **URL Name** text box, enter a tenant URL name that matches the tenant URL name in the source environment.
   
   The URL name is used to append a tenant-specific identifier to the vRealize Automation console URL.
   
   For example, if the URL name for DEVTenant in the source environment is dev, enter **dev** to create the URL https://vra-va-hostname.domain.name/vcac/org/dev.
6. (Optional) Enter an email address in the **Contact Email** text box.
7. Click **Submit and Next**.
Create an Administrator for Each Added Tenant

You must create an administrator for each tenant that you added to the target environment. You create an administrator by creating a local user account and assigning tenant administrator privileges to the local user account.

Perform this procedure for each tenant in your target environment.

Prerequisites

- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Log in to the target vRealize Automation console as Administrator with the password you entered when you deployed the target vRealize Automation appliance.

Note For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

Procedure

1. Select Administration > Tenants.
2. Click a tenant that you added.
   For example, for DEVTenant, click DEVTenant.
3. Click Local users.
4. Click the New icon (➕).
5. In User Details, enter the requested information to create a local user account to assign the tenant administrator role.
   The local user name must be unique to the default local directory, vsphere.local.
6. Click OK.
7. Click Administrators.
8. Enter the local user name in the Tenant administrators search box and press Enter.
9. Click the appropriate name in the search returns to add the user to the list of tenant administrators.
10. Click Finish.
11. Log out of the console.

What to do next

- For a minimal deployment: Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment.
For a high-availability deployment: Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment.

Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment

Before you import your users and groups to a minimal deployment of vRealize Automation, you must connect the target vRealize Automation to your Active Directory link.

Perform this procedure for each tenant. If a tenant has more than one Active Directory, perform this procedure for each Active Directory that the tenant uses.

Prerequisites

- Create an Administrator for Each Added Tenant.
- Verify that you have access privileges to the Active Directory.
- Log in to vRealize Automation as a tenant administrator.

Procedure

1. Select Administration > Directories Management > Directories.
2. Click Add Directory icon (⊕) and select Add Active Directory over LDAP/IWA.
3. Enter your Active Directory account settings.

   ✦ For Non-Native Active Directories

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name.</td>
</tr>
<tr>
<td></td>
<td>Select Active Directory over LDAP when using Non-Native Active Directory.</td>
</tr>
<tr>
<td>This Directory Supports DNS Service Location</td>
<td>Deselect this option.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the distinguished name (DN) of the starting point for directory server searches.</td>
</tr>
<tr>
<td></td>
<td>For example, cn=users,dc=rainpole,dc=local.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>Enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.</td>
</tr>
<tr>
<td></td>
<td>For example, cn=config_admin infra,cn=users,dc=rainpole,dc=local.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory password for the account that can search for users and click Test Connection to test the connection to the configured directory.</td>
</tr>
</tbody>
</table>

   ✦ For Native Active Directories

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name.</td>
</tr>
<tr>
<td></td>
<td>Select Active Directory (Integrated Windows Authentication) when using Native Active Directory.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the name of the domain to join.</td>
</tr>
<tr>
<td>Domain Admin Username</td>
<td>Enter the user name for the domain admin.</td>
</tr>
<tr>
<td>Domain Admin Password</td>
<td>Enter the password for the domain admin.</td>
</tr>
<tr>
<td>Option</td>
<td>Sample Input</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bind User UPN</td>
<td>Use the email address format to enter the name of the user who can authenticate with the domain.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory bind account password for the account that can search for users.</td>
</tr>
</tbody>
</table>

4. Click **Save & Next**.

**Select the Domains** displays a list of domains.

5. Accept the default domain setting and click **Next**.

6. Verify that the attribute names are mapped to the correct Active Directory attributes, and click **Next**.

7. Select the groups and users to synchronize.
   a. Click the **New** icon (➕).
   b. Enter the user domain and click **Find Groups**.
      For example, enter `dc=vcac, dc=local`.
   c. To select the groups to synchronize, click **Select** and click **Next**.
   d. On **Select Users**, select the users to synchronize and click **Next**.
      Only add users and groups that are required to use vRealize Automation. Do not select **Sync nested groups** unless all of the groups in the nest are required to use vRealize Automation.

8. Review the users and groups you are syncing to the directory, and click **Sync Directory**.
   The directory synchronization takes some time and runs in the background.

**What to do next**

*Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment*

Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment

Before you import your users and groups to a high-availability vRealize Automation environment, you must connect to your Active Directory link.

- Perform steps 1-8 for each tenant. If a tenant has more than one Active Directory, perform this procedure for each Active Directory that the tenant uses.
- Repeat steps 9–10 for each identity provider associated with a tenant.

**Prerequisites**

- **Create an Administrator for Each Added Tenant.**
- Verify that you have access privileges to the Active Directory.
- Log in to vRealize Automation as a tenant administrator.
Procedure

1. Select Administration > Directories Management > Directories.
2. Click Add Directory icon ( ) and select Add Active Directory over LDAP/IWA.
3. Enter your Active Directory account settings.

   − For Non-Native Active Directories

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name.</td>
</tr>
<tr>
<td></td>
<td>Select Active Directory over LDAP when using Non-Native Active Directory.</td>
</tr>
<tr>
<td>This Directory Supports DNS Service Location</td>
<td>Deselect this option.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the distinguished name (DN) of the starting point for directory server searches.</td>
</tr>
<tr>
<td></td>
<td>For example, cn=users,dc=rainpole,dc=local.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>Enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.</td>
</tr>
<tr>
<td></td>
<td>For example, cn=config_admin infra,cn=users,dc=rainpole,dc=local.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory password for the account that can search for users and click Test Connection to test the connection to the configured directory.</td>
</tr>
</tbody>
</table>

   − For Native Active Directories

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name.</td>
</tr>
<tr>
<td></td>
<td>Select Active Directory (Integrated Windows Authentication) when using Native Active Directory.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the name of the domain to join.</td>
</tr>
<tr>
<td>Domain Admin Username</td>
<td>Enter the user name for the domain admin.</td>
</tr>
<tr>
<td>Domain Admin Password</td>
<td>Enter the password for the domain admin account.</td>
</tr>
<tr>
<td>Bind User UPN</td>
<td>Use the email address format to enter the name of the user who can authenticate with the domain.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory bind account password for the account that can search for users.</td>
</tr>
</tbody>
</table>

4. Click Save & Next.

   The Select the Domains page displays the list of domains.
5. Accept the default domain setting and click Next.
6. Verify that the attribute names are mapped to the correct Active Directory attributes, and click Next.
Select the groups and users to synchronize.

a. Click the **New** icon.

b. Enter the user domain and click **Find Groups**.
   
   For example, enter `dc=vcac,dc=local`.

c. To select the groups to synchronize, click **Select** and click **Next**.

d. On the **Select Users** page, select the users to synchronize and click **Next**.

Only add users and groups that are required to use vRealize Automation. Do not select **Sync nested groups** unless all of the groups in the nest are required to use vRealize Automation.

Review the users and groups you are syncing to the directory, and click **Sync Directory**.

The directory synchronization takes some time and runs in the background.

Select **Administration > Directories Management > Identity Providers**, and click your new identity provider.

For example, **WorkspaceIDP__1**.

On the page for the identity provider that you selected, add a connector for each node.

a. Follow the instructions for **Add a Connector**.

b. Update the value for the **IdP Hostname** property to point to the fully qualified domain name (FQDN) for the vRealize Automation load balancer.

c. Click **Save**.

**What to do next**

Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.

Before you migrate, you must run NSX Network and Security Inventory data collection in the source vRealize Automation environment.

This data collection is necessary for the Load Balancer Reconfigure action to work in vRealize Automation 7.4 when you migrate from 7.1, 7.2, or 7.3 deployments.

**Note** You do not need to run this data collection in your source environment when you migrate from vRealize Automation 6.2.x. vRealize Automation 6.2.x does not support the Load Balancer Reconfigure action.

**Procedure**

- Run NSX Network and Security Inventory data collection in your source vRealize Automation environment before you migrate to vRealize Automation 7.4. See **Start Endpoint Data Collection Manually** in Managing vRealize Automation.
What to do next

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.

Before migration, you must back up your IaaS Microsoft SQL database in the vRealize Automation source environment and restore it to a new blank database created in the vRealize Automation target environment.

Prerequisites

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.
- Obtain information about backing up and restoring an SQL Server database. Find articles on the Microsoft Developer Network about creating a full SQL Server database backup and restoring an SQL Server database to a new location.

Procedure

- Create a full backup of your source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database. You use the backup to restore the SQL database to a new blank database created in the target environment.

What to do next

Snapshot the Target vRealize Automation Environment.

Take a snapshot of each target vRealize Automation virtual machine. If migration is unsuccessful, you can try again using the virtual machine snapshots.

For information, see your vSphere documentation.

Prerequisites

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.

What to do next

Perform one of the following procedures:

- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment.
- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

Migration Procedures

The procedure you perform to migrate your source vRealize Automation environment data depends on whether you migrate to a minimal environment or to a high-availability environment.

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4.
All tenants in the source system must be recreated in the target and go through the Migrate Identity Stores procedure. For more information, see Migrate Identity Stores to VMware Identity Manager.

**Prerequisites**

- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment.
- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as root using the password you entered when you deployed the target vRealize Automation appliance.

**Procedure**

1. Select **vRA Settings > Migration**.

2. Enter the information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name for the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the vRealize Automation appliance.</td>
</tr>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created.</td>
</tr>
</tbody>
</table>

3. Enter the information for the target vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the target vRealize Automation appliance.</td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local You cannot modify this field.</td>
</tr>
<tr>
<td>Administrator username</td>
<td>administrator You cannot modify this field.</td>
</tr>
<tr>
<td>Administrator password</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>
4 Enter the information for the target IaaS database server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>The location of the Microsoft SQL Server where the restored vRealize Automation IaaS Microsoft SQL database resides. If a named instance and a non-default port are used, enter in <code>SERVER,PORT.INSTANCE-NAME</code> format. If you configure the target Microsoft SQL Server to use the AlwaysOn Availability Group (AAG) feature, the target SQL Server should be entered as the AAG listener name, without a port or instance name.</td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.</td>
</tr>
<tr>
<td>Authentication mode</td>
<td>If you use the Windows authentication mode, the IaaS service user must have the SQL Server db_owner role. The same permissions apply when using SQL Server authentication mode.</td>
</tr>
<tr>
<td></td>
<td>SQL Server opens the Login name and Password text boxes.</td>
</tr>
<tr>
<td>Login name</td>
<td>Login name of the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.</td>
</tr>
<tr>
<td>Original encryption key</td>
<td>Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment.</td>
</tr>
<tr>
<td>New passphrase</td>
<td>A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>

5 Click **Validate**.

The page displays the validation progress.

- If all the items validate successfully, go to step 8.
- If an item fails to validate, inspect the error message and the validation log file on the IaaS nodes. For log file locations, see Migration Log Locations. Click **Edit Settings** and edit the problem item. Go to step 7.

6 Click **Migrate**.

The page displays the migration progress.

- If migration is successful, the page displays all migration tasks as completed.
- If migration is unsuccessful, inspect the migration log files on the virtual appliance and the IaaS nodes. For log file locations, see Migration Log Locations.

Finish these steps before you restart migration.

- Revert your target vRealize Automation environment to the state you captured when you took a snapshot before migration.
b Restore your target IaaS Microsoft SQL database using the backup of the source IaaS database.

What to do next

Post-Migration Tasks.

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4 configured as a high-availability environment.

All tenants in the source system must be recreated in the target and go through the Migrate Identity Stores procedure. For more information, see Migrate Identity Stores to VMware Identity Manager.

Prerequisites

- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment.
- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as root using the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1. Select vRA Settings > Migration.

2. Enter the information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name for the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the source vRealize Automation appliance.</td>
</tr>
</tbody>
</table>

3. Enter the information for the migration package location on the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created.</td>
</tr>
</tbody>
</table>
4 Enter the information for the target vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the target vRealize Automation appliance.</td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>Administrator username</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>

5 Enter the information for the target IaaS database server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>The location of the Microsoft SQL Server instance where the restored vRealize Automation IaaS Microsoft SQL database resides. If a named instance and a non-default port are used, enter in <code>SERVER,PORT\INSTANCE-NAME</code> format. If you configure the target Microsoft SQL Server to use the AlwaysOn Availability Group (AAG) feature, the target SQL Server should be entered as the AAG listener name, without a port or instance name.</td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.</td>
</tr>
</tbody>
</table>
| Authentication mode     | - **Windows**<br>  If you use the Windows authentication mode, the IaaS service user must have the SQL Server `db_owner` role. The same permissions apply when using SQL Server authentication mode.  
  - **SQL Server**<br>  SQL Server opens the Login name and Password text boxes. |
| Login name              | Login name of the SQL Server user with the `db_owner` role for the cloned IaaS Microsoft SQL database. |
| Password                | Password for the SQL Server user with the `db_owner` role for the cloned IaaS Microsoft SQL database. |
| Original encryption key | Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment. |
| New passphrase          | A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment. |

6 Click **Validate**.

The page displays the validation progress.

- If all the items validate successfully, go to step 8.
- If an item fails to validate, inspect the error message and the validation log file on the IaaS nodes. For log file locations, see Migration Log Locations. Click **Edit Settings** and edit the problem item. Go to step 7.
7 Click **Migrate**.

The page displays the migration progress.
- If migration is successful, the page displays all migration tasks as completed.
- If migration is unsuccessful, inspect the migration log files on the virtual appliance and the IaaS nodes. For log file locations, see **Migration Log Locations**.

Finish these steps before you restart migration.

- Revert your target vRealize Automation environment to the state you captured when you took a snapshot before migration.
- Restore your target IaaS Microsoft SQL database using the backup of the source IaaS database.

**What to do next**

**Post-Migration Tasks.**

**Post-Migration Tasks**

After you migrate vRealize Automation, perform the post-migration tasks that pertain to your situation.

**Note** After you migrate the identity stores, users of vRealize Code Stream must manually reassign vRealize Code Stream roles.

**Add Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment**

You must delete and restore the vRealize Automation 6.2.x tenant administrators in each tenant after migration.

Perform the following procedure for each tenant in the target vRealize Automation console.

**Note** If you migrate from a vRealize Automation 7.x environment, you do not need to perform this procedure.

**Prerequisites**

- Successful migration to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console as **Administrator** with the password you entered when you deployed the target vRealize Automation appliance.

**Procedure**

1. Select **Administration > Tenants**.
2. Click a tenant name.
3. Click **Administrators**.
4. Make a list of each tenant administrator name and user name.
5. Point to each administrator and click the delete icon (Delete) until you delete all administrators.
6. Click **Finish**.
7 On the Tenants page, click the tenant name again.

8 Click **Administrators**.

9 Enter the name of each user that you deleted in the appropriate search box and press Enter.

10 Click the name of the appropriate user from the search returns to add the user back as an administrator.

   When you finish, the list of tenant administrators looks the same as the list of administrators you deleted.

11 Click **Finish**.

Run Test Connection and Verify Migrated Endpoints

Migrating to vRealize Automation 7.4 makes changes to endpoints in the target environment.

After you migrate to vRealize Automation 7.4, you must use the **Test Connection** action for all applicable endpoints. You might also need to make adjustments to some migrated endpoints. For more information, see Considerations When Working With Upgraded or Migrated Endpoints.

The default security setting for upgraded or migrated endpoints is not to accept untrusted certificates.

After upgrading or migrating from an earlier vRealize Automation installation, if you were using untrusted certificates you must perform the following steps for all vSphere and NSX endpoints to enable certificate validation. Otherwise, the endpoint operations fail with certificate errors. For more information, see VMware Knowledge Base articles *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* at http://kb.vmware.com/kb/2150230 and *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* at http://kb.vmware.com/kb/2108294.

1 After upgrade or migration, log in to the vRealize Automation vSphere agent machine and restart your vSphere agents by using the **Services** tab.

   Migration might not restart all agents, so manually restart them if needed.

2 Wait for at least one ping report to finish. It takes a minute or two for a ping report to finish.

3 When the vSphere agents have started data collection, log in to vRealize Automation as an IaaS administrator.

4 Click **Infrastructure > Endpoints > Endpoints**.

5 Edit a vSphere endpoint and click **Test Connection**.

6 If a certificate prompt appears, click **OK** to accept the certificate.

   If a certificate prompt does not appear, the certificate might currently be correctly stored in a trusted root authority of the Windows machine hosting service for the endpoint, for example as a proxy agent machine or DEM machine.

7 Click **OK** to apply the certificate acceptance and save the endpoint.

8 Repeat this procedure for each vSphere endpoint.

9 Repeat this procedure for each NSX endpoint.
If the **Test Connection** action is successful but some data collection or provisioning operations fail, you can install the same certificate on all the agent machines that serve the endpoint and on all DEM machines. Alternatively, you can uninstall the certificate from existing machines and repeat the preceding procedure for the failing endpoint.

### Run NSX Network and Security Inventory Data Collection in Your Target vRealize Automation 7.4 Environment

After you migrate, you must run NSX Network and Security Inventory data collection in the target vRealize Automation 7.4 environment.

This data collection is necessary for the Load Balancer Reconfigure action to work in vRealize Automation 7.4 for 7.1, 7.2, and 7.3 deployments.

**Note** You do not need to perform this data collection if you migrated from vRealize Automation 6.2.x to 7.4.

### Prerequisites

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.
- Successfully migrate to vRealize Automation 7.4.

### Procedure


### Reconfigure Load Balancers After Migration to a High-Availability Environment

When you migrate to a high-availability environment, you must perform these tasks for each load balancer after you finish migration.

**Prerequisites**

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

### Procedure

1. Restore the original health check settings so replica nodes can accept incoming traffic by configuring the load balancers for these items.
   - vRealize Automation appliance.
   - IaaS Web Server that hosts the Model Manager.
   - Manager Service.
2. Change the load balancer timeout settings back to the default.

### Migrating an External Orchestrator Server to vRealize Automation 7.4

You can migrate your existing external Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation.
You can deploy vRealize Orchestrator as an external server instance and configure vRealize Automation to work with that external instance, or you can configure and use the vRealize Orchestrator server that is included in the vRealize Automation appliance.

VMware recommends that you migrate your external vRealize Orchestrator to the Orchestrator server that is built into vRealize Automation. The migration from an external to embedded Orchestrator provides the following benefits:

- Reduces the total cost of ownership.
- Simplifies the deployment model.
- Improves the operational efficiency.

**Note** Consider using the external vRealize Orchestrator in the following cases:

- Multiple tenants in the vRealize Automation environment.
- Geographically dispersed environment.
- Workload handling.
- Use of specific plug-ins, such as the Site Recovery Manager plug-in versions earlier than 6.5.

**Migration Scenarios**

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

**Migration Scenario Matrix**

You can choose a migration scenario based on the source deployment.

<table>
<thead>
<tr>
<th>vRealize Orchestrator Deployment</th>
<th>vRealize Automation Deployment</th>
<th>Migration Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Orchestrator 6.0.3 Virtual Appliance</td>
<td>vRealize Automation 6.2.3</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.4 on Windows</td>
<td>vRealize Automation 6.2.4</td>
<td>Migrate an External vRealize Orchestrator 6.x on Windows to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.4 Virtual Appliance</td>
<td>vRealize Automation 6.2.4</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.5 Virtual Appliance</td>
<td>vRealize Automation 6.2.5</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12c</td>
<td>vRealize Automation 7.0 or IaaS</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator Deployment</td>
<td>vRealize Automation Deployment</td>
<td>Migration Scenario</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database</td>
<td>vRealize Automation 7.0.1 or IaaS</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.1 Virtual Appliance</td>
<td>vRealize Automation 7.1</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.2 Virtual Appliance</td>
<td>vRealize Automation 7.2</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.3 Virtual Appliance</td>
<td>vRealize Automation 7.3</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.3 on Windows</td>
<td>vRealize Automation 6.2.3</td>
<td>Migrate the Orchestrator Configuration from Windows to Virtual Appliance</td>
</tr>
</tbody>
</table>

Migrate the Orchestrator Configuration from Windows to Virtual Appliance

Migrate your 5.5.x and 6.x Orchestrator Windows standalone configuration to the Orchestrator Appliance.

**Prerequisites**

- Deploy and configure an Orchestrator node on the target version. See Configuring a Standalone Orchestrator Server.
- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.
- Stop the Orchestrator server service on both the source and the target Orchestrator instances.
- Back up the source Orchestrator database, including the database schema.

**Note** If you plan to preserve the source Orchestrator environment after migration, clone the source Orchestrator database to another database. Afterwards, configure the target Orchestrator to use the cloned instance, instead of the instance configured during installation. If you skip this step, the target Orchestrator will upgrade the source Orchestrator database and it will no longer work with the source Orchestrator environment.

**Procedure**

1. Download the migration tool from the target Orchestrator server.
   a. Log in to Control Center as `root`.
   b. Open the Export/Import Configuration page and click the Import Configuration tab.
   c. Download the migration tool as specified in the description on the page, or download it directly from https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool.
2 Export the Orchestrator configuration from the source Orchestrator server.
   a Extract the downloaded archive in the Orchestrator install folder.
      The default path to the Orchestrator install folder in a Windows-based installation is C:\Program
      Files\VMware\Orchestrator.
   b Set the PATH environment variable by pointing it to the bin folder of the Java JRE installed with
      Orchestrator.
   c Use the Windows command prompt to navigate to the bin folder under the Orchestrator install
      folder.
      By default, the path to the bin folder is C:\Program
      Files\VMware\Orchestrator\migration-cli\bin.
   d Run the export command from the command line.
      
      C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export

      This command combines the VMware vRealize Orchestrator configuration files and plug-ins into
      an export archive.
      An archive with file name orchestrator-config-export-orchestrator_ip_address-
      date_hour.zip is created in the same folder as the migration-cli folder.

3 Import the configuration to the target Orchestrator instance.
   a Log in to Control Center as root.
   b Open Export/Import Configuration in Control Center and click the Import Configuration tab.
   c Browse to and select the .ZIP file exported from the source Orchestrator instance.
   d Enter the password that you used when exporting the configuration.
      Leave blank if you did not export the configuration with a password.
   e Select the import type.
   f If you are importing the configuration to an external Orchestrator server, choose whether to import
      the database settings.
      
      **Note** If the source and target Orchestrator servers are not configured to use the same external
      database, leave the Migrate database settings check box unselected to avoid upgrading the
      database schema to the newer version. Otherwise the source Orchestrator environment stops
      working.
      You must configure the database that the target Orchestrator will use before the migration.
   g Click IMPORT to finish the migration.
      A message states that the configuration is successfully imported. The Orchestrator server service
      of the target Orchestrator instance restarts automatically.
If the target vRealize Orchestrator uses an authentication provider server that is different from the one used by the source Orchestrator, import to the trust store of the target Orchestrator the SSL certificate of the authentication provider it is configured to use.

a On the Certificates page in Control Center, click Import from URL.

b Provide the URL of the vRealize Automation or vSphere instance.

A message indicates that the migration finished successfully. The Orchestrator server service restarts automatically.

What to do next
Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

Migrate an External vRealize Orchestrator 6.x on Windows to vRealize Automation 7.4
After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x installed on Windows to the Orchestrator server that is built into vRealize Automation 7.4.

Note If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

Prerequisites
- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see Upgrading vRealize Automation in Installing or Upgrading vRealize Automation.
- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

Procedure
1 Download the migration tool from the target Orchestrator server.
   a Log in to the vRealize Automation appliance over SSH as root.
   b Download the migration-tool.zip archive that is located in the /var/lib/vco/downloads directory.
2 Export the Orchestrator configuration from the source Orchestrator server.
   a Set the PATH environment variable by pointing it to the bin folder of the Java JRE installed with Orchestrator.
   b Upload the migration tool to the Windows server, on which the external Orchestrator is installed.
c Extract the downloaded archive in the Orchestrator install folder.
   The default path to the Orchestrator install folder in a Windows-based installation is C:\Program Files\VMware\Orchestrator.

d Run the Windows command prompt as administrator and navigate to the bin folder in the Orchestrator install folder.
   By default, the path to the bin folder is C:\Program Files\VMware\Orchestrator\migration-cli\bin.

e Run the export command from the command line.
   C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
   This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.
   The archive is created in the same folder as the migration-cli folder.

3 Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.
a On the vRealize Automation appliance, stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.
   service vco-server stop && service vco-configurator stop

b Upload the exported configuration file to the /usr/lib/vco/tools/configuration-cli/bin directory on the vRealize Automation appliance.

c Change the ownership of the exported Orchestrator configuration file.
   chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip

d Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the vro-configure script with the import command.
   ./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip

e Remove all certificates from the database keystore.
   ./vro-configuration.sh untrust --reset-db
4 Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the db-migrate command.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Note** Enclose passwords that contain special characters in single quotation marks.

The JDBC_connection_URL depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th>database_name</th>
<th>vmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>database_user</td>
<td>vmware</td>
</tr>
<tr>
<td>database_user_password</td>
<td>vmware</td>
</tr>
</tbody>
</table>

You successfully migrated an external vRealize Orchestrator 6.x installed on Windows to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

**What to do next**

Set up the built-in vRealize Orchestrator server. See [Configure the Built-In vRealize Orchestrator Server](#).

**Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4**

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x Virtual Appliance to the Orchestrator server that is built into vRealize Automation 7.4.

**Note** If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see [Upgrading vRealize Automation](#).
- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.
- Stop the Orchestrator server service of the external Orchestrator.
Back up the database, including the database schema, of the external Orchestrator server.

**Procedure**

1. **Download the migration tool from the target Orchestrator server to the source Orchestrator.**
   - a. Log in to the vRealize Orchestrator 6.x Virtual Appliance over SSH as **root**.
   - b. Under the `/var/lib/vco` directory, run the `scp` command to download the migration-tool.zip archive.
     ```bash
     scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
     ```
   - c. Run the `unzip` command to extract the migration tool archive.
     ```bash
     unzip migration-tool.zip
     ```

2. **Export the Orchestrator configuration from the source Orchestrator server.**
   - a. In the `/var/lib/vco/migration-cli/bin` directory, run the export command.
     ```bash
     ./vro-migrate.sh export
     ```
     This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.
     An archive with file name `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` is created in the `/var/lib/vco` folder.

3. **Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.**
   - a. Log in to the vRealize Automation appliance over SSH as **root**.
   - b. Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.
     ```bash
     service vco-server stop && service vco-configurator stop
     ```
   - c. Under the `/usr/lib/vco/tools/configuration-cli/bin` directory, run the `scp` command to download the exported configuration archive.
     ```bash
     scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
     ```
d Change the ownership of the exported Orchestrator configuration file.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

e Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the vro-configure script with the import command.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

4 If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.

a In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.

b Set the values of `listen_addresses` to a wildcard (`*`).

```
listen_addresses = '*'
```

c Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.

```
host all all vra-va-ip-address/32 md5
```

**Note** The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.

d Restart the PostgreSQL server service.

```
service vpostgres restart
```
5 Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the db-migrate command.

```bash
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Note** Enclose passwords that contain special characters in single quotation marks.

The `JDBC_connection_URL` depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th><code>database_name</code></th>
<th><code>vmware</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>

6 Remove all certificates from the database keystore.

```bash
./vro-configure.sh untrust --reset-db
```

7 Reinstall the Orchestrator plug-ins.
   a Log in to Control Center as root.
   b Click Troubleshooting.
   c Click Force plug-ins reinstall.

8 Start the Orchestrator server service.

9 Revert to the default configuration of the `postgresql.conf` and the `pg_hba.conf` file.
   a Restart the PostgreSQL server service.

You successfully migrated an external vRealize Orchestrator 6.x Virtual Appliance to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

**What to do next**

Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server. Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4.
You can export the configuration from your existing external Orchestrator instance and import it to the Orchestrator server that is built into vRealize Automation.

**Note** If you have multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**
- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see *Upgrading vRealize Automation* in *Installing or Upgrading vRealize Automation*.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

**Procedure**

1. Export the configuration from the external Orchestrator server.
   a. Log in to Control Center of the external Orchestrator server as **root** or as an **administrator**, depending on the source version.
   b. Stop the Orchestrator server service from the **Startup Options** page to prevent unwanted changes to the database.
   c. Go to the **Export/Import Configuration** page.
   d. On the **Export Configuration** page, select **Export server configuration**, **Bundle plug-ins** and **Export plug-in configurations**.

2. Migrate the exported configuration into the embedded Orchestrator instance.
   a. Upload the exported Orchestrator configuration file to the `/usr/lib/vco/tools/configuration-cli/bin` directory of the vRealize Automation appliance.
   b. Log in to the vRealize Automation appliance over SSH as **root**.
   c. Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

   ```bash
   service vco-server stop && service vco-configurator stop
   ```
   
   d. Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

   ```bash
   ./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
   ```
3 If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.
   a In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.
   b Set the values of `listen_addresses` to a wildcard ("*").
   ```plaintext
   listen_addresses = '*'
   ```
   c Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.
   ```plaintext
   host all all vra-va-ip-address/32 md5
   ```
   Note The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.
   d Restart the PostgreSQL server service.
   ```plaintext
   service vpostgres restart
   ```

4 Migrate the database to the internal PostgreSQL database, by running the `vro-configure` script with the `db-migrate` command.
   ```plaintext
   .vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
   ```
   Note Enclose passwords that contain special characters in single quotation marks.

The `JDBC_connection_URL` depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th><code>database_name</code></th>
<th><code>vmware</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>
5 Remove all certificates from the database keystore.

./vro-configuration.sh untrust --reset-db

6 Reinstall the Orchestrator plug-ins.
   a Log in to Control Center as root.
   b Click Troubleshooting.
   c Click Force plug-ins reinstall.

7 Start the Orchestrator server service.

8 Revert to the default configuration of the postgresql.conf and the pg_hba.conf file.
   a Restart the PostgreSQL server service.

You successfully migrated an external Orchestrator server instance to a vRealize Orchestrator instance embedded in vRealize Automation.

What to do next
Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

Configure the Built-In vRealize Orchestrator Server
After you export an external vRealize Orchestrator configuration and import it to vRealize Automation, you configure the vRealize Orchestrator server that is built into vRealize Automation.

Prerequisites
Migrate the configuration from the external to the internal vRealize Orchestrator.

Procedure
1 Log in as root to a command prompt session on the vRealize Automation appliance.
2 Start services for the vRealize Orchestrator Control Center and server:

   service vco-configurator start && service vco-server start

3 Log in as root to the built-in vRealize Orchestrator Control Center.

   https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config

   Note  You can skip the next step when the external and internal vRealize Orchestrator versions are the same.

4 In Control Center, click Validate Configuration, and verify that vRealize Orchestrator is configured properly.

5 In Control Center, click Certificates, click Package Signing Certificate, and generate a new package signing certificate.
In Control Center, click **Configure Authentication Provider**.

**Default tenant** and **Admin group** are set to default values `vsphere.local` and `vsphere.local\vcoadmins`. Change the defaults to the values for your environment.

In the vRealize Automation appliance management interface, under **Services**, verify that `vco-server` is **REGISTERED**.

Select the `vco` services of the external vRealize Orchestrator server, and click **Unregister**.

**What to do next**

- Import any certificates that were trusted in the external vRealize Orchestrator server to the trust store of the built-in vRealize Orchestrator. For more information, see *Manage Orchestrator Certificates*.

- Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the vRealize Orchestrator configuration.

  For more information, see *Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability in Installing or Upgrading vRealize Automation*.

  **Note** The vRealize Orchestrator instances are automatically clustered and available for use.

- Restart the `vco-configurator` service on all nodes in the cluster.

- Update the vRealize Orchestrator endpoint to point to the migrated built-in vRealize Orchestrator server.

- Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.

**Update Embedded vRealize Orchestrator to Trust vRealize Automation Certificates**

If you update or change vRealize Automation appliance or IaaS certificates, you must update vRealize Orchestrator to trust the new or updated certificates.

This procedure applies to all vRealize Automation deployments that use an embedded vRealize Orchestrator instance. If you use an external vRealize Orchestrator instance, see *Update External vRealize Orchestrator to Trust vRealize Automation Certificates*.

**Note** This procedure resets tenant and group authentication back to the default settings. If you have customized your authentication configuration, note your changes so that you can re-configure authentication after completing the procedure.

See the vRealize Orchestrator documentation for information about updating and replacing vRealize Orchestrator certificates.

If you replace or update vRealize Automation certificates without completing this procedure, the vRealize Orchestrator Control Center may be inaccessible, and errors may appear in the `vco-server` and `vco-configurator` log files.

Problems with updating certificates can also occur if vRealize Orchestrator is configured to authenticate against a different tenant and group than vRealize Automation. See [https://kb.vmware.com/kb/2147612](https://kb.vmware.com/kb/2147612).
Procedure

1. Stop the vRealize Orchestrator server and Control Center services.
   
   ```
   service vco-server stop
   service vco-configurator stop
   ```

2. Reset the vRealize Orchestrator authentication provider.
   
   a. Run the `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication` command.
   
   b. Delete `/etc/vco/app-server/vco-registration-id`.
   
   c. Run `vcac-vami vco-service-reconfigure`

3. Start the vRealize Orchestrator server and control center services.
   
   ```
   service vco-server start
   service vco-configurator start
   ```

Control Center Differences Between External and Embedded Orchestrator

Some of the menu items that are available in Control Center of an external vRealize Orchestrator are not included in the default Control Center view of an embedded Orchestrator instance.

In Control Center of the embedded Orchestrator server, a few options are hidden by default.

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.</td>
</tr>
<tr>
<td>Export/Import Configuration</td>
<td>The embedded Orchestrator configuration is included in the exported vRealize Automation components.</td>
</tr>
<tr>
<td>Configure Database</td>
<td>The embedded Orchestrator uses the database that is used by vRealize Automation.</td>
</tr>
<tr>
<td>Customer Experience Improvement Program</td>
<td>You can join the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance management interface. See The Customer Experience Improvement Program in Managing vRealize Automation.</td>
</tr>
</tbody>
</table>

Another options that are hidden from the default Control Center view are the Host address text box and the UNREGISTER button on the Configure Authentication Provider page.

**Note**  To see the full set of Control Center options in vRealize Orchestrator that is built into vRealize Automation, you must access the advanced Orchestrator Management page at `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/?advanced` and click the F5 button on the keyboard to refresh the page.

Reconfigure the vRealize Automation Endpoint in the Target vRealize Orchestrator

Use the following procedure to reconfigure the vRealize Automation endpoint in the embedded target vRealize Orchestrator.
Prerequisites

- Successful migration to the latest version of vRealize Automation.
- Connect to the target vRealize Orchestrator using the vRealize Orchestrator client. For information, see Using the VMware vRealize Orchestrator Client in the vRealize Orchestrator documentation.

Procedure

1. Select Design from the top drop-down menu.
2. Click Inventory.
3. Expand vRealize Automation.
4. If you migrated from a minimal environment, identify endpoints containing the fully qualified domain name (FQDN) of the source vRealize Automation appliance host. If you migrated from a high-availability environment, identify endpoints containing the FQDN of the source appliance load balancer.

<table>
<thead>
<tr>
<th>If you find endpoints containing the FQDN, complete these steps.</th>
<th>If you do not find endpoints containing the FQDN, complete these steps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click Workflows. 2. Click the expand button to select Library &gt; vRealize Automation &gt; Configuration. 3. Do one of these steps.</td>
<td>1. Click Resources. 2. Click the update icon on the top toolbar. 3. Click the expand button to select Library &gt; vCACCAFE &gt; Configuration. 4. Do one of these steps.</td>
</tr>
<tr>
<td>- If you migrated from a minimal environment, run the Remove a vRA host workflow for every endpoint containing the FQDN of the source vRealize Automation appliance host.  - If you migrated from a high-availability environment, run the Remove a vRA host workflow for every endpoint containing the FQDN of the source appliance load balancer.</td>
<td>- If you migrated from a minimal environment, delete each resource that has a URL property containing the FQDN of the source vRealize Automation appliance host.  - If you migrated from a high-availability environment, delete each resource that has a URL property containing the FQDN of the source vRealize Automation appliance load balancer.</td>
</tr>
</tbody>
</table>

5. Click Workflows.
6. Click the expand button to select Library > vRealize Automation > Configuration.
7. To add the target vRealize Automation appliance host or if you migrated to a high-availability deployment, the load-balanced host, run the Add a vRA host using component registry workflow.

Reconfigure the vRealize Automation Infrastructure Endpoint in the Target vRealize Orchestrator

Use the following procedure to reconfigure the vRealize Automation infrastructure endpoint in the embedded target vRealize Orchestrator.

Prerequisites

- Successful migration to the latest version of vRealize Automation.
- Connect to the target vRealize Orchestrator using the vRealize Orchestrator client. For information, see Using the VMware vRealize Orchestrator Client in the vRealize Orchestrator documentation.
**Procedure**

1. Select **Design** from the top drop-down menu.
2. Click **Inventory**.
3. Expand **vRealize Automation Infrastructure**.
4. If you migrated from a minimal environment, identify endpoints containing the fully qualified domain name (FQDN) of the source vRealize Automation infrastructure host. If you migrated from a high-availability environment, identify endpoints containing the FQDN of the source appliance load balancer.

<table>
<thead>
<tr>
<th>If you find endpoints containing the FQDN, complete these steps.</th>
<th>If you do not find endpoints containing the FQDN, complete these steps.</th>
</tr>
</thead>
</table>
| 1. Click **Workflows**.  
2. Click the expand button to select Library > vRealize Automation > Infrastructure Administration > Configuration.  
3. Do one of these steps.  
   - If you migrated from a minimal environment, run the **Remove an IaaS host** workflow for every endpoint containing the FQDN of the source vRealize Automation infrastructure host.  
   - If you migrated from a high-availability environment, run the **Remove an IaaS host** workflow for every endpoint containing the FQDN of the source vRealize Automation infrastructure host load balancer. | 1. Click **Resources**.  
2. Click the update icon on the top toolbar.  
3. Click the expand button to select Library > vCAC > Configuration.  
4. Do one of these steps.  
   - If you migrated from a minimal environment, delete each resource that has a host property containing the FQDN of the source vRealize Automation infrastructure host.  
   - If you migrated from a high-availability environment, delete each resource that has a host property containing the FQDN of the source vRealize Automation infrastructure host load balancer. |

5. Click **Workflows**.
6. Click the expand button to select Library > vRealize Automation > Configuration.
7. To add the target vRealize Automation infrastructure host, or if you migrated to a high-availability deployment load-balanced host, run the **Add the IaaS host of a vRA host** workflow.

**Install vRealize Orchestrator Customization**

You can run a workflow to install the customized state change workflow stubs and vRealize Orchestrator menu operation workflows.

For information, see [Install vRealize Orchestrator Customization](#).

**Prerequisites**

Successful migration to the latest version of vRealize Automation.

**Reconfigure Embedded vRealize Orchestrator Infrastructure Endpoint in the Target vRealize Automation**

When you migrate from a vRealize Automation 6.2.x environment, you must update the URL of the infrastructure endpoint that points to the target embedded vRealize Orchestrator server.
Prerequisites

- Successfully migrate to vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  
  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.
  
  For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.
  
  b. Log in as a IaaS administrator user.

Procedure

1. Select **Infrastructure > Endpoints > Endpoints**.
2. On the Endpoints page, select the vRealize Orchestrator endpoint, and click **Edit**.
3. In the Address text box, edit the vRealize Orchestrator endpoint URL.
   
   a. If you migrated to a minimal environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-hostname.domain.name:443/vco.
   
   b. If you migrated to a high-availability environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-lb-hostname.domain.name:443/vco.
4. Click **OK**.
5. Manually run a data collection on the vRealize Orchestrator endpoint.
   
   a. On the Endpoints page, select the vRealize Orchestrator endpoint.
   
   b. Select **Actions > Data Collection**.
   
   Verify that the data collection is successful.

Reconfigure the Azure Endpoint in the Target vRealize Automation Environment

After migration, you must reconfigure your Microsoft Azure endpoint.

Perform this procedure for each Azure endpoint.

Prerequisites

- Successfully migrate to the latest version of vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  
  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.
  
  For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.
  
  b. Log in as a IaaS administrator user.
Procedure

1. Select Administration > vRO Configuration > Endpoints.
2. Select an Azure endpoint.
3. Click Edit.
4. Click Details.
5. In the Client secret text box, enter the original client secret.
6. Click Finish.
7. Repeat for each Azure endpoint.

Migrate vRealize Automation 6.2.x Automation Application Services to 7.4

You can use the VMware vRealize Application Services Migration Tool to migrate your existing application services blueprints and deployment profiles from VMware vRealize Application Services 6.2.x to vRealize Automation 7.4.

Prerequisites

Successful migration to the latest version of vRealize Automation.

Procedure

♦ To download the VMware vRealize Application Services Migration Tool, complete these steps.
  a. Click Download VMware vRealize Automation.
  b. Select Drivers & Tools > VMware vRealize Application Services Migration Tool.

Delete Original Target vRealize Automation IaaS Microsoft SQL Database

You can delete the original IaaS database after migration is complete.

Prerequisites

Successful migration to the latest version of vRealize Automation.

Your migrated environment does not use the original vRealize Automation IaaS Microsoft SQL database that you created when you installed the target vRealize Automation environment. You can safely delete this original IaaS database from the Microsoft SQL Server after you complete migration.

Update Data Center Location Menu Contents After Migration

After migration, you must add any missing custom data center locations to the Location drop-down menu.

After migration to the latest version of vRealize Automation, the data center locations in the Location drop-down menu on the Compute Resources page revert to the default list. Although custom data center locations are missing, all compute resource configurations migrate successfully and the Vrm.DataCenter.Location property is not affected. You can still add custom data center locations to the Location menu.
Prerequisites

Migrate to the latest version of vRealize Automation.

Procedure

- Add missing data center locations to the Location drop-down menu. See Scenario: Add Datacenter Locations for Cross Region Deployments.

Upgrading Software Agents to TLS 1.2

After you migrate to vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4, you must perform several tasks to upgrade the Software Agents from your source environment to Transport Layer Security (TLS) 1.2.

Beginning with vRealize Automation 7.4, TLS 1.2 is the only supported TLS protocol for data communication between vRealize Automation and your browser. After migration, you must upgrade existing virtual machine templates from your vRealize Automation 7.1 or 7.3 source environment as well as any existing virtual machines.

Update Source Environment Virtual Machine Templates

You must update existing vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 templates after you complete migration to 7.4 so that the Software Agents use the TLS 1.2 protocol.

Guest agent and agent bootstrap code must be updated in the source environment templates. If you are using a linked clone option, you might need to remap the templates with the newly created virtual machines and their snapshots.

To upgrade your templates, you complete these tasks.

1. Log in to vSphere.
2. Convert each template from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to a virtual machine and power on the machine.
3. Import the appropriate software installer and run the software installer on each virtual machine.
4. Convert each virtual machine back to a template.

Use this procedure to locate the software installers for Linux or Windows.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.

Procedure

1. Start a browser and open the vRealize Automation 7.4 appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.
2. Click Guest and software agents page.
3. Follow the instructions for the Linux or Windows software installers.

What to do next

Identify Virtual Machines that Need Software Agent Upgrade.
Identify Virtual Machines that Need Software Agent Upgrade

You can use the Health Service in the vRealize Automation Console to identify virtual machines that need software agent update to TLS 1.2.

Sometimes the patch applied to your vRealize Automation source environment does not upgrade all of the virtual machines. You can use the Health Service to identify the virtual machines that still need a software agent update to TLS 1.2. All software agents in the target environment need to be updated for post-provisioning procedures.

Prerequisites

- **Apply Software Agent Patch** if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- You have successfully migrated vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You are logged in to vRealize Automation 7.4 on the primary virtual appliance.

Procedure

1. Click **Administration > Health**.
2. Click **New Configuration**.
3. On the Configuration Details page, provide the requested information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter <strong>SW Agent verification</strong></td>
</tr>
<tr>
<td>Description</td>
<td>Add optional description, for example, <strong>Locate software agents for upgrade to TLS 1.2</strong></td>
</tr>
<tr>
<td>Product</td>
<td>Select vRealize Automation 7.4.0.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Select None.</td>
</tr>
</tbody>
</table>

4. Click **Next**.
5. On the Select Test Suites page, select **System Tests for vRealize Automation** and **Tenant Tests for vRealize Automation**.
6. Click **Next**.
7. On the Configure Parameters page, provide the requested information.

**Table 1-66. vRealize Automation Virtual Appliance**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Public Web Server Address | For a minimal deployment, the base URL for the vRealize Automation appliance host. For example, https://va-host.domain/.  
                         | For a high-availability deployment, the base URL for the vRealize Automation load balancer. For example, https://load-balance-host.domain/. |
| SSH Console Address     | Fully qualified domain name of the vRealize Automation appliance. For example, va-host.domain.                                               |
### Table 1-66. vRealize Automation Virtual Appliance (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Console User</td>
<td>root</td>
</tr>
<tr>
<td>SSH Console Password</td>
<td>Password for root.</td>
</tr>
<tr>
<td>Max Service Response Time (ms)</td>
<td>Accept default: 2000</td>
</tr>
</tbody>
</table>

### Table 1-67. vRealize Automation System Tenant

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tenant Administrator</td>
<td>administrator</td>
</tr>
<tr>
<td>System Tenant Password</td>
<td>Password for administrator.</td>
</tr>
</tbody>
</table>

### Table 1-68. vRealize Automation Disk Space Monitoring

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning Threshold Percent</td>
<td>Accept default: 75</td>
</tr>
<tr>
<td>Critical Threshold Percent</td>
<td>Accept default: 90</td>
</tr>
</tbody>
</table>

### Table 1-69. vRealize Automation Tenant

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant Under Test</td>
<td>Tenant selected for testing.</td>
</tr>
<tr>
<td>Fabric Administrator User Name</td>
<td>Fabric administrator user name. For example, <a href="mailto:admin@va-host.local">admin@va-host.local</a>.</td>
</tr>
<tr>
<td></td>
<td>Note This fabric administrator must also have a tenant administrator and an IaaS administrator role in order for all of the tests to run.</td>
</tr>
<tr>
<td>Fabric Administrator Password</td>
<td>Password for fabric administrator.</td>
</tr>
</tbody>
</table>

8 Click **Next**.

9 On the Summary page, review the information and click **Finish**.

The software agent verification configuration is finished.

10 On the SW Agent verification card, click **Run**.

11 When the test is complete, click the center of the SW Agent verification card.

12 On the SW Agent verification results page, page through the test results and find the Check Software Agent Version test in the Name column. If the test result is Failed, click the **Cause** link in the Cause column to see the virtual machines with an outdated software agent.

**What to do next**

If you have virtual machines with an outdated software agent, see Upgrade Software Agents on vSphere.

Upgrade Software Agents on vSphere
You can upgrade any outdated Software Agents on vSphere to TLS 1.2 after migration using vRealize Automation Appliance Management.

This procedure updates the outdated Software Agents on the virtual machines from your source environment to TLS 1.2 and is required for migration to vRealize Automation 7.4.

**Prerequisites**
- **Apply Software Agent Patch** if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You have used Health Service to identify virtual appliances with outdated Software Agents.

**Procedure**

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as **root** using the password you entered when you deployed the vRealize Automation appliance.  
   For a high-availability environment, open Appliance Management on the master appliance.

2. Click **vRA Settings > SW Agents**.

3. Click **Toggle TLS 1.0, 1.1**.
   
   TLS v1.0, v1.1 Status is ENABLED.

4. For Tenant credentials, enter the requested information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant name</td>
<td>Name of tenant on the source vRealize Automation appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The tenant user must have the Software Architect role assigned.</td>
</tr>
<tr>
<td>Username</td>
<td>Tenant administrator user name on the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>Tenant administrator password.</td>
</tr>
</tbody>
</table>

5. Click **Test connection**.
   
   If a connection is established, a success message appears.

6. For Source appliance, enter the IP address or fully qualified domain name of the source vRealize Automation appliance.
   
   The source and the target appliance must both use the same tenant credentials.

7. Click **List batches**.
   
   The Batch Choice List table appears.
8 Click Show.

A table appears with a list of virtual machines with outdated Software Agents.

9 Upgrade the Software Agent for the virtual machines that are in the UPGRADABLE state.

- To upgrade the Software Agent in an individual virtual machine, click Show for a group of virtual machines, identify the virtual machine you want to upgrade and click Run to start the upgrade process.
- To upgrade the Software Agent for a batch of virtual machines, identify the group that you want to upgrade and click Run to start the upgrade process.

If you have more than 200 virtual machines to upgrade, you can control the batch upgrade process speed by entering values for these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Queue Depth</td>
<td>The number of parallel upgrade executions that take place at one time. For example, 20. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Batch Errors</td>
<td>The REST error count causing batch upgrade to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Failures</td>
<td>The number of failed Software Agent upgrades causing batch processing to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Polling</td>
<td>How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.</td>
</tr>
</tbody>
</table>

If the upgrade process is too slow or produces too many unsuccessful upgrades, you can adjust these parameters to improve upgrade performance.

**Note** Clicking Refresh clears the list of batches. It does not affect the upgrade process. It also refreshes information about whether TLS 1.2 is set or not. In addition, clicking Refresh also performs a health check of vRealize Automation services. If services are not running, the system displays an error message and inactivates all other action buttons.

10 Click Toggle TLS 1.0, 1.1.

TLS v1.0, v1.1 Status is DISABLED.

Upgrade Software Agents on Amazon Web Service or Azure

You can upgrade outdated Software Agents on Amazon Web Service (AWS) or Azure manually.

- You must update the tunnel properties specified in the reservation of the migrated vRealize Automation server.
Prerequisites

- **Apply Software Agent Patch** if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- A software tunnel is present and the tunnel virtual machine IP address is known.

Procedure

1. Create a node file for each node that you need to upgrade.

   ```bash
   /usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
   ```

2. Create a plan file to upgrade the Software Agent on a Linux or a Windows virtual machine.

   - Modify the migrate params file under /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} to contain the value of the private IP address corresponding to the AWS or Azure endpoint.

     ```json
     "key": "ipAddress",
     "value": {
       "type": "string",
       "value": "<$PrivateIp:$PrivatePort>"
     }
     ```

   - Use this command for updating a Linux machine.

     ```bash
     ```

   - Use this command for updating a Windows machine.

     ```bash
     ```

   - This command runs the plan file.

     ```bash
     ```
3 Use this command to update the Software Agent using the node file from step 1 and the plan file from step 2.

```
```

As an alternative, you can use this command to run one node at a time from the node file by providing a node index.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

As you perform this procedure, you can tail logs from the vRealize Automation virtual appliance and host machine to see the Server Agent upgrade process.

After upgrade, the upgrade process imports a software update script for Windows or Linux to the vRealize Automation 7.4 virtual appliance. You can log into the vRealize Automation virtual appliance host to ensure that the software component is imported successfully. After the component is imported, a software update is sent to the old Event Broker Service (EBS) to relay software update scripts to the identified virtual machines. When the upgrade completes and the new Software Agents become operative, they bind to the new vRealize Automation virtual appliance by sending a ping request.

**Note** Useful Log Files

- Catalina output for source vRealize Automation: `/var/log/vcac/catalina.out`. In this file, you see the upgrade requests being made as the agent migrations are made. This activity is the same as running a software provisioning request.

- Catalina output for destination vRealize Automation: `/var/log/vcac/catalina.out`. In this file, you see the migrated virtual machines reporting their ping requests here to include version numbers 7.4.0- SNAPSHOT. You can tally these together by comparing the EBS topic names, for example, sw-agent-UUID.

- Agent update folder on destination vRealize Automation machine master upgrade log file: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. You can tail this file to see which upgrade operation is in progress.

- Individual logs available under tenant folders: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Individual nodes are listed here as lot files with failures and in-progress extensions.

- Migrated VMs: `/opt/vmware-appdirector/agent/logs/darwin*.log`. You can spot check this location which should list the software update requests being received as well as the eventual restart of the agent_bootstrap + software agent.
Change Property Dictionary Setting After Migration from 6.2.5

The Label control in the vRealize Automation 6.2.x property dictionary does not exist in the vRealize Automation 7.x property dictionary.

During migration to vRealize Automation 7.4 or earlier, the Label control is converted to a TextBox control type in the migrated property dictionary.

During migration to vRealize Automation 7.5 or later, the Label control is converted to a TextArea control type in the migrated property dictionary. The TextArea control type supports long label names better than the TextBox control type used when migrating to earlier versions of vRealize Automation 7.x.

After migration, you can set property definitions that contain an impacted TextBox or TextArea control type as not overridable, either manually in each blueprint's vRealize Automation properties settings, manually in each blueprint component, reservation, endpoint and so on in which an impacted custom property definition is used, or programmatically by using export and import capabilities in vRealize CloudClient.

Procedure

1. After migration and to determine which property definitions use a TextBox (7.4 and earlier) or TextArea (7.5 or later) type control, click Administration > Property Definitions and view the Display Area setting for each property definition of the String data type. These are the property definitions to set as not overrideable in your migrated vRealize Automation instance.

2. Set impacted custom properties as not overrideable.
   - Manually for the overall blueprint
     1. Click the Design tab and open a blueprint.
     2. Click the gear icon to open the Blueprint Properties page.
     3. Click the Properties tab on the Blueprint Properties page and click Custom Properties.
     4. Toggle Overrideable off for all property definitions that contain a TextBox or TextArea control type.
   - Manually for each blueprint component, reservation, endpoint and so on in which an impacted custom property is used
     1. For endpoints and reservation, click Infrastructure and select either Endpoints or Reservations.
     2. Open each target element and use its Properties tab to set the impacted TextBox (7.4 and earlier) or TextArea (7.5 or later) type control as not overrideable.
     3. Open each blueprint and use the Properties tab in each machine, network, and other component in the blueprint canvas to update any impacted property definitions.
Programmatically for the overall blueprint

1. Export the blueprint by using a vRealize CloudClient export command sequence.

2. Mark the impacted property definitions as not overrideable. In this example, TestLabel is set to not overrideable and TestOverrideLabel is set in a way that it can be edited on a request form.

TestLabel:
- fixed: default test label description at BP
- required: true
- secured: false
- visible: true

TestOverrideLabel:
- default: override this value
- required: true
- secured: false
- visible: true

3. Import the blueprint by using a vRealize CloudClient import command sequence.

Validate the Target vRealize Automation 7.4 Environment

You can verify that all data is migrated successfully to the target vRealize Automation environment.

Prerequisites

- Migrate to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console.

  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.

  For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

  b. Log in with the tenant administrator user name and password.

Procedure

1. Select **Infrastructure > Managed Machines** and verify that all the managed virtual machines are present.

2. Click **Compute Resources**, select each endpoint, and click **Data Collection, Request now**, and **Refresh** to verify that the endpoints are working.

3. Click **Design**, and on the **Blueprints** page, verify the elements of each blueprint.

4. Click **XaaS** and verify the contents of **Custom Resources, Resource Mappings, XaaS Blueprints**, and **Resource Actions**.

5. Select **Administration > Catalog Management** and verify the contents of **Services, Catalog Items, Actions**, and **Entitlements**.

6. Select **Items > Deployments** and verify the details for the provisioned virtual machines.
7 On the Deployments page, select a provisioned, powered off, virtual machine and select Actions > Power On, click Submit, and click OK. Verify that the virtual machine powers on correctly.

8 Click Catalog and request a new catalog item.

9 On the General tab, enter the request information.

10 Click the Machine icon, accept all the default settings, click Submit, and click OK.

11 Verify that the request finishes successfully.

Troubleshooting Migration

Migration troubleshooting topics provide solutions to problems you might experience when you migrate vRealize Automation.

PostgreSQL Version Causes Error

A source vRealize Automation 6.2.x environment containing an updated PostgreSQL database blocks administrator access.

Problem

If an upgraded PostgreSQL database is used by vRealize Automation 6.2.x, an administrator must add an entry to the pg_hba.conf file that provides access to this database from vRealize Automation.

Solution

1 Open the pg_hba.conf file.

2 To grant access to this database, add the following entry.

   host all vcac-database-user vra-va-ip trust-method

Some Virtual Machines Do Not Have a Deployment Created during Migration

Virtual machines in the missing state at the time of migration do not have a corresponding deployment created in the target environment.

Problem

If a virtual machine is in the missing state in the source environment during migration, a corresponding deployment is not created in the target environment.

Solution

If a virtual machine goes out of the missing state after migration, you can import the virtual machine to the target deployment using bulk import.

Migration Log Locations

You can troubleshoot validation or migration problems by viewing the logs that record the migration process.

Table 1-70. Source vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package creation log</td>
<td>/var/log/vmware/vcac/migration-package.log</td>
</tr>
</tbody>
</table>
Table 1-71. Target vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration log</td>
<td>/var/log/vmware/vcac/migrate.log</td>
</tr>
<tr>
<td>Migration execution log</td>
<td>/var/log/vmware/vcac/mseq.migration.log</td>
</tr>
<tr>
<td>Migration execution output log</td>
<td>/var/log/vmware/vcac/mseq.migration.out.log</td>
</tr>
<tr>
<td>Validation execution log</td>
<td>/var/log/vmware/vcac/mseq.validation.log</td>
</tr>
<tr>
<td>Validation execution output log</td>
<td>/var/log/vmware/vcac/mseq.validation.out.log</td>
</tr>
</tbody>
</table>

Table 1-72. Target vRealize Automation Infrastructure Nodes

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration log</td>
<td>C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log</td>
</tr>
<tr>
<td>Validation log</td>
<td>C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log</td>
</tr>
</tbody>
</table>

Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request

Catalog items that use certain property definitions from prior versions appear in the service catalog but are not available to request after migrating to the latest version of vRealize Automation.

Problem

If you migrated from a 6.2.x or earlier version and you had property definitions with these control types or attributes, these elements are missing from the property definitions and any catalog items that use the definitions do not function as they did before you performed the migration.

- Control types. Check box or link.
- Attributes. Relationship, regular expressions, or property layouts.

Cause

In vRealize Automation 7.0 and later, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes.

Migrate the control type or attributes to vRealize Automation 7.x using a script action.

Solution

1. In vRealize Orchestrator, create a script action that returns the property values. The action must return a simple type. For example, return strings, integers, or other supported types. The action can take the other properties on which it depends as an input parameter.

2. In vRealize Automation console, configure the product definition.
   b. Select the property definition and click Edit.
   c. From the Display advice drop-down menu, select Dropdown.
From the Values drop-down menu, select External Values.

Select the script action.

Click OK.

Configure the Input Parameters that are included in the script action. To preserve the existing relationship, bind the parameter to the other property.

Click OK.

Data Collection Radio buttons Disabled in vRealize Automation

After migration from vRealize Automation 6.2.x to 7.x, the Compute Resources page on the target vRealize Automation contains disabled radio buttons under Data Collection.

Cause

If you install an agent on the source environment that points to an endpoint and install an agent on the target environment that points to the same endpoint but the agent has a different name, you can run a test connection to the endpoint as administrator in the target environment. However, if you log in to vRealize Automation on the target environment as a fabric administrator, the radio buttons on the Compute Resources page under Data Collection are disabled.

Solution

Avoid this situation by giving the name of the agent installed on the target environment the same name as the agent installed on the source environment.

Troubleshooting the Software Agent Upgrade

When you use vRealize Automation Appliance Management to upgrade software agents, you can review log files to identify the cause of any problems you experience.

Problem

You might experience problems when you upgrade the software agents. By observing the log files during the software agent upgrade process, you can identify where there is a problem.

Note  Server Logs

- Tail the updateSoftwareAgents.log file on the server to observe the process: /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log.
- Tail the catalina.out file on target appliance to see which software agents are succeeding: /var/log/vcac/catalina.out.
  - Look for s string such as "ping" reported back for 7.4.0-SNAPSHOT.

You can find additional information at these locations.

- /var/cache/vcac/agentupdate/[Tenant]/[UUID]/UUID.plan
- /var/cache/vcac/agentupdate/[Tenant]/[UUID]/UUID.log
- /var/cache/vcac/agentupdate/sqa/UUID/UUID.log (per OS)
Before you start a major batch upgrade, you should always perform a test virtual appliance software agent upgrade. For an overview of the process:

- Observe the first request made to the target virtual appliance to identify the agent versions.
- Observe the request made to the source virtual appliance for upgrade.
- Observe the agents reporting their new 7.4 version in the target virtual appliance.
- Between these events, observe the updateSoftwareAgents.log file at /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log

**Note**  Client Logs

Linux agent logs are in appdirector agent logs folder: /opt/vmware-appdirector/agent/logs/*.log

You might see log errors like these, which are temporary because the EBS queues go out and in during the upgrade process.


org.springframework.web.client.HttpClientErrorException: 404 Not Found

at org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]

**Enable Your Load Balancers**

If your deployment uses load balancers, re-enable secondary nodes and health checks and revert the load balancer timeout settings.
The health checks for vRealize Automation vary according to version. For information, see the *vRealize Automation Load Balancing Configuration Guide* in the *VMware vRealize Automation Documentation*.

Change the load balancer timeout settings from 10 minutes back to the default.

**Post-Upgrade Tasks for Upgrading vRealize Automation**

After you upgrade from vRealize Automation 7.1, or later, you must perform required post-upgrade tasks.

**Upgrading Software Agents to TLS 1.2**

After you upgrade to vRealize Automation 7.4, you must perform several tasks to upgrade the Software Agents from your vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 environment to TLS 1.2.

Beginning with vRealize Automation 7.4, Transport Layer Security (TLS) 1.2 is the only supported TLS protocol for data communication between vRealize Automation and your browser.

After migration, you must upgrade existing virtual machine templates from your vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 environment as well as any existing virtual machines.

**Update vRealize Automation Virtual Machine Templates**

You must update existing templates after you complete upgrade to vRealize Automation 7.4 so that the Software Agents use the TLS 1.2 protocol.

Guest agent and agent bootstrap code must be updated in the templates from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1. If you are using a linked clone option, you might need to remap the templates with the newly created virtual machines and their snapshots.

To upgrade your templates, you complete these tasks.

1. Log in to vSphere.
2. Convert each template from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to a virtual machine and power on the machine.
3. Import the appropriate software installer and run the software installer on each virtual machine.
4. Convert each virtual machine back to a template.

Use this procedure to locate the software installer for Linux or Windows.

**Prerequisites**

Successful upgrade to vRealize Automation 7.4.

**Procedure**

1. Start a browser and open the vRealize Automation 7.4 appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.
2. Click *Guest and software agents page*.
3. Follow the instructions for the Linux or Windows software installer.
What to do next

Identify Virtual Machines that Need Software Agent Upgrade.

Identify Virtual Machines that Need Software Agent Upgrade

You can use the Health Service in vRealize Automation to identify virtual machines that need a Software Agent update to TLS 1.2.

You can use the Health Service to identify the virtual machines that need a Software Agent update to TLS 1.2. All Software Agents in the vRealize Automation 7.4 environment need to be updated so that you can perform post-provisioning procedures, which require secure communication between your browser and vRealize Automation.

Prerequisites

- You have successfully upgraded to vRealize Automation 7.4.
- You are logged in to vRealize Automation 7.4 on the primary virtual appliance as tenant administrator.

Procedure

1. Click **Administration > Health**.
2. Click **New Configuration**.
3. On the Configuration Details page, provide the requested information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter <strong>SW Agent verification</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Add optional description, for example,</td>
</tr>
<tr>
<td></td>
<td><strong>Locate software agents for upgrade to TLS 1.2.</strong></td>
</tr>
<tr>
<td>Product</td>
<td>Select vRealize Automation 7.4.0.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Next**.
5. On the Select Test Suites page, select **System Tests for vRealize Automation** and **Tenant Tests for vRealize Automation**.
6. Click **Next**.
7 On the Configure Parameters page, provide the requested information.

**Table 1-73. vRealize Automation Virtual Appliance**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Public Web Server Address  | For a minimal deployment, the base URL for the vRealize Automation appliance host. For example, https://va-host.domain/.  
For a high-availability deployment, the base URL for the vRealize Automation load balancer. For example, https://load-balancer-host.domain/. |
| SSH Console Address        | Fully qualified domain name of the vRealize Automation appliance. For example, va-host.domain. |
| SSH Console User           | root        |
| SSH Console Password       | Password for root. |
| Max Service Response Time (ms) | Accept default: 2000 |

**Table 1-74. vRealize Automation System Tenant**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tenant Administrator</td>
<td>administrator</td>
</tr>
<tr>
<td>System Tenant Password</td>
<td>Password for administrator.</td>
</tr>
</tbody>
</table>

**Table 1-75. vRealize Automation Disk Space Monitoring**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning Threshold Percent</td>
<td>Accept default: 75</td>
</tr>
<tr>
<td>Critical Threshold Percent</td>
<td>Accept default: 90</td>
</tr>
</tbody>
</table>

**Table 1-76. vRealize Automation Tenant**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant Under Test</td>
<td>Tenant selected for testing.</td>
</tr>
</tbody>
</table>
| Fabric Administrator User Name | Fabric administrator user name. For example, admin@va-host.local.  
*Note* This fabric administrator must also have a tenant administrator and an IaaS administrator role in order for all of the tests to run. |
| Fabric Administrator Password | Password for fabric administrator. |

8 Click **Next**.

9 On the Summary page, review the information and click **Finish**.

The software agent verification configuration is finished.

10 On the SW Agent verification card, click **Run**.

11 When the test is complete, click the center of the SW Agent verification card.
12 On the SW Agent verification results page, page through the test results and find the Check Software Agent Version test in the Name column. If the test result is Failed, click the **Cause** link in the Cause column to see the virtual machines with an outdated software agent.

**What to do next**

If you have virtual machines with an outdated software agent, see Upgrade Software Agents on vSphere.

**Upgrade Software Agents on vSphere**

You can upgrade outdated Software Agents on vSphere to TLS 1.2 after upgrade using vRealize Automation Appliance Management.

This procedure updates the outdated Software Agents to TLS 1.2 on the virtual machines in your upgraded environment. It is required for upgrade to vRealize Automation 7.4.

**Prerequisites**

- Successful upgrade to vRealize Automation 7.4.
- You have used Health Service to identify virtual appliances with outdated Software Agents.

**Procedure**

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as **root** using the password you entered when you deployed the vRealize Automation appliance.

   For a high-availability environment, open Appliance Management on the master appliance.

2. Click **vRA Settings > SW Agents**.

3. Click **Toggle TLS 1.0, 1.1**.

   TLS v1.0, v1.1 Status is **ENABLED**.

4. For Tenant credentials, enter the requested information for the vRealize Automation 7.4 appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant name</td>
<td>Name of tenant on the upgraded vRealize Automation appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The tenant user must have the Software Architect role assigned.</td>
</tr>
<tr>
<td>Username</td>
<td>Tenant administrator user name on the vRealize Automation appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>Tenant administrator password.</td>
</tr>
</tbody>
</table>

5. Click **Test connection**.

   If a connection is established, a success message appears.

6. Click **List batches**.

   The Batch Choice List table appears.
7 Click **Show**.

A table appears with a list of virtual machines with outdated Software Agents.

8 Upgrade the Software Agent for the virtual machines that are in the UPGRADABLE state.

- To upgrade the Software Agent in an individual virtual machine, click **Show** for a group of virtual machines, identify the virtual machine you want to upgrade and click **Run** to start the upgrade process.

- To upgrade the Software Agent for a batch of virtual machines, identify the group that you want to upgrade and click **Run** to start the upgrade process.

If you have more than 200 virtual machines to upgrade, you can control the batch upgrade process speed by entering values for these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Queue Depth</td>
<td>The number of parallel upgrade executions that take place at one time. For example, 20. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Batch Errors</td>
<td>The REST error count causing batch upgrade to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Failures</td>
<td>The number of failed Software Agent upgrades causing batch processing to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Polling</td>
<td>How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.</td>
</tr>
</tbody>
</table>

If the upgrade process is too slow or produces too many unsuccessful upgrades, you can adjust these parameters to improve upgrade performance.

**Note** Clicking **Refresh** clears the list of batches. It does not affect the upgrade process. It also refreshes information about whether TLS 1.2 is set or not. In addition, clicking **Refresh** also performs a health check of vRealize Automation services. If services are not running, the system displays an error message and inactivates all other action buttons.

9 Click **Toggle TLS 1.0, 1.1**.

TLS v1.0, v1.1 Status is DISABLED.

**Upgrade Software Agents on Amazon Web Service or Azure**

You can upgrade any outdated Software Agents on virtual machines on Amazon Web Service (AWS) or Azure manually.
Prerequisites

- Successful upgrade to vRealize Automation 7.4.
- A software tunnel is present and the tunnel virtual machine IP address is known.

Procedure

1. Create a node file for each node that you need to upgrade.

   ```
   /usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
   ```

   **Note** For an in-place upgrade, the $DestinationVRAServer is the same as the $SourceVRAServer.

2. Create a plan file to upgrade the Software Agent on a Linux or a Windows virtual machine.

   - Modify the migrate params file under /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} to contain the value of the private IP address corresponding to the AWS or Azure endpoint.

     ```
     "key": "ipAddress",
     "value": {
       "type": "string",
       "value": "<$PrivateIp:$PrivatePort>"
     }
     ```

   - Use this command for updating a Linux machine.

     ```
     ```

   - Use this command for updating a Windows machine.

     ```
     ```

   - This command runs the plan file.

     ```
     ```
3 Use this command to update the Software Agent using the node file from step 1 and the plan file from step 2.

```
```

As an alternative, you can use this command to run one node at a time from the node file by providing a node index.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

As you perform this procedure, you can tail logs from the vRealize Automation virtual appliance and host machine to see the Server Agent upgrade process.

After upgrade, the upgrade process imports a software update script for Windows or Linux to the vRealize Automation 7.4 virtual appliance. You can log into the vRealize Automation virtual appliance host to ensure that the software component is imported successfully. After the component is imported, a software update is sent to the old Event Broker Service (EBS) to relay software update scripts to the identified virtual machines. When the upgrade completes and the new Software Agents become operative, they bind to the new vRealize Automation virtual appliance by sending a ping request.

**Note** Useful Log Files

- **Catalina output for source vRealize Automation**: /var/log/vcac/catalina.out. In this file, you see the upgrade requests being made as the agent migrations are made. This activity is the same as running a software provisioning request.
- **Catalina output for destination vRealize Automation**: /var/log/vcac/catalina.out. In this file, you see the migrated virtual machines reporting their ping requests here to include version numbers 7.4.0-SNAPSHOT. You can tally these together by comparing the EBS topic names, for example, sw-agent-UUID.
- **Agent update folder on destination vRealize Automation machine master upgrade log file**: /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. You can tail this file to see which upgrade operation is in progress.
- **Individual logs available under tenant folders**: /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}. Individual nodes are listed here as lot files with failures and in-progress extensions.
- **Migrated VMs**: /opt/vmware-appdirector/agent/logs/darwin*.log. You can spot check this location which should list the software update requests being received as well as the eventual restart of the agent_bootstrap + software agent.
Set the vRealize Automation PostgreSQL Replication Mode to Synchronous

If you set the PostgreSQL replication mode to asynchronous before upgrade, you can set the PostgreSQL replication mode to synchronous after you upgrade a distributed vRealize Automation environment.

Prerequisites
- You have upgraded a distributed vRealize Automation environment.
- You are logged in as root to the appropriate vRealize Automation Appliance Management at https://vra-va-hostname.domain.name:5480.

Procedure
1. Click vRA Settings > Database.
2. Click Sync Mode and wait until the action completes.
3. Verify that all nodes in the Sync State column display Sync status.

What to do next
Run Test Connection and Verify Upgraded Endpoints.

Run Test Connection and Verify Upgraded Endpoints

Upgrading from vRealize Automation 7.3 or earlier to 7.4 makes changes to endpoints in the target environment.

After you upgrade to vRealize Automation 7.4, you must use the Test Connection action for all applicable endpoints. You might also need to make adjustments to some upgraded endpoints. For more information, see Considerations When Working With Upgraded or Migrated Endpoints.

The default security setting for upgraded or migrated endpoints is not to accept untrusted certificates.

After upgrading or migrating from an earlier vRealize Automation installation, if you were using untrusted certificates you must perform the following steps for all vSphere and NSX endpoints to enable certificate validation. Otherwise, the endpoint operations fail with certificate errors. For more information, see VMware Knowledge Base articles Endpoint communication is broken after upgrade to vRA 7.3 (2150230) at http://kb.vmware.com/kb/2150230 and How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294) at http://kb.vmware.com/kb/2108294.

1. After upgrade or migration, log in to the vRealize Automation vSphere agent machine and restart your vSphere agents by using the Services tab.
   Migration might not restart all agents, so manually restart them if needed.
2. Wait for at least one ping report to finish. It takes a minute or two for a ping report to finish.
3. When the vSphere agents have started data collection, log in to vRealize Automation as an IaaS administrator.
4. Click Infrastructure > Endpoints > Endpoints.
5. Edit a vSphere endpoint and click Test Connection.
6 If a certificate prompt appears, click **OK** to accept the certificate.

   If a certificate prompt does not appear, the certificate might currently be correctly stored in a trusted root authority of the Windows machine hosting service for the endpoint, for example as a proxy agent machine or DEM machine.

7 Click **OK** to apply the certificate acceptance and save the endpoint.

8 Repeat this procedure for each vSphere endpoint.

9 Repeat this procedure for each NSX endpoint.

If the **Test Connection** action is successful but some data collection or provisioning operations fail, you can install the same certificate on all the agent machines that serve the endpoint and on all DEM machines. Alternatively, you can uninstall the certificate from existing machines and repeat the preceding procedure for the failing endpoint.

### Run NSX Network and Security Inventory Data Collection After You Upgrade from vRealize Automation

After you upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4, you must run NSX Network and Security Inventory data collection in the vRealize Automation 7.4 environment.

This data collection is necessary for the load balancer reconfigure action to work in vRealize Automation 7.4 for 7.1, 7.2, or 7.3.x deployments.

**Prerequisites**

- Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.
- Successful upgrade to vRealize Automation 7.4.

**Procedure**

- Run NSX Network and Security Inventory data collection in vRealize Automation 7.4 after you upgrade. See Start Endpoint Data Collection Manually.

### Join Replica Appliance to Cluster

After you complete the master vRealize Automation appliance update, each updated replica node is automatically joined to the master node. In case a replica node has to be separately updated, use these steps to manually join the replica node to the cluster.

Access the appliance management console of the replica node that is not joined to the cluster and perform the following steps.

**Procedure**

1 Select **vRA Settings > Cluster**.

2 Click **Join Cluster**.
Port Configuration for High-Availability Deployments

After finishing an upgrade in a high-availability deployment, you must configure the load balancer to pass traffic on port 8444 to the vRealize Automation appliance to support remote console features.

For more information, see the vRealize Automation Load Balancing Configuration Guide in the vRealize Automation Documentation.

Reconfigure the Built-In vRealize Orchestrator to Support High Availability

For a high-availability deployment, you must manually rejoin each target replica vRealize Automation appliance to the cluster to enable high-availability support for the embedded vRealize Orchestrator.

Prerequisites

Log in to the target replica vRealize Automation appliance management console.

1. Start a browser and open the target replica vRealize Automation management console using the fully qualified domain name (FQDN) of the target replica virtual appliance: https://vra-va-hostname.domain.name:5480.
2. Log in with the user name root and the password that you entered when you deployed the target replica vRealize Automation appliance.

Procedure

1. Select vRA Settings > Cluster.
2. In the Leading Cluster Node text box, enter the FQDN of the target master vRealize Automation appliance.
3. Enter the root password in the Password text box.
4. Click Join Cluster.
   Continue past any certificate warnings. The system restarts services for the cluster.
5. Verify that the services are running.
   a. On the top tab bar, click Services.
   b. Click Refresh to monitor the progress of services startup.

Restore External Workflow Timeout Files

You must reconfigure the vRealize Automation external workflow timeout files because the upgrade process overwrites xmldb files.

Procedure

1. Open the external workflow configuration (xmldb) files on your system from the following directory. \VMware\vCAC\Server\ExternalWorkflows\xmldb\.
2. Replace the xmldb files with the files that you backed up before migration. If you do not have backup files, reconfigure the external workflow timeout settings.
3. Save your settings.
Restore Changes to Logging in the app.config File

The upgrade process overwrites changes you make to logging in the configuration files. After you finish an upgrade, you must restore any changes you made before the upgrade to the app.config file.

Enable Automatic Manager Service Failover After Upgrade

Automatic Manager Service failover is disabled by default when you upgrade vRealize Automation. Complete these steps to enable automatic Manager Service after upgrade.

Procedure

1. Open a command prompt as root on the vRealize Automation appliance.
3. To enable automatic Manager Service failover, run the following command.
   
   python ./manager-service-automatic-failover ENABLE

   To disable automatic failover throughout an IaaS deployment, run the following command.
   
   python ./manager-service-automatic-failover DISABLE

About Automatic Manager Service Failover

You can configure the vRealize Automation IaaS Manager Service to automatically fail over to a backup if the primary Manager Service stops.

Starting in vRealize Automation 7.3, you no longer need to manually start or stop the Manager Service on each Windows server, to control which serves as primary or backup. Automatic Manager Service failover is disabled by default when you upgrade IaaS with the Upgrade Shell Script or using the IaaS Installer executable file.

When automatic failover is enabled, the Manager Service automatically starts on all Manager Service hosts, including backups. The automatic failover feature allows the hosts to transparently monitor each other and fail over when necessary, but the Windows service must be running on all hosts.

Note  You are not required to use automatic failover. You may disable it and continue to manually start and stop the Windows service to control which host serves as primary or backup. If you take the manual failover approach, you must only start the service on one host at a time. With automatic failover disabled, simultaneously running the service on multiple IaaS servers makes vRealize Automation unusable.

Do not attempt to selectively enable or disable automatic failover. Automatic failover must always be synchronized as on or off, across every Manager Service host in an IaaS deployment.

Import DynamicTypes Plug-In

If you are using the DynamicTypes plug-in, and you exported the configuration as a package before the upgrade, you must import the following workflow.

1. Import Dynamic Types Configuration in the target environment.
   
   a. Log in to the Java Client as administrator.
b Select the **Workflows** tab.

c Select **Library > Dynamic Types > Configuration**.

d Select the **Import Configuration From Package** workflow and run it.

e Click **Configuration package to import**.

f Browse to the exported package file and click **Attach file**.

g Review the information about the namespaces attached to the package and click **Submit**.

2 Select **Inventory > Dynamic Types** to verify that the dynamic type namespaces have been imported.

**Troubleshooting the vRealize Automation Upgrade**

The upgrade troubleshooting topics provide solutions to problems that you might encounter when upgrading vRealize Automation from 7.1, 7.2, or 7.3.x to 7.4.

**Automatic Manager Service Failover Does Not Activate**

Suggestions for troubleshooting manager-service-automatic-failover command.

**Solution**

- The manager-service-automatic-failover command fails or displays this message for more than two minutes: **Enabling Manager Service automatic failover mode on node: IAAS_MANAGER_SERVICE_NODEID**.

  a Log in to vRealize Automation appliance management at https://va-hostname.domain.name:5480 with the user name **host** and the password you entered when you deployed the appliance.

  b Select **vRA Settings > Cluster**.

  c Verify that the Management Agent service is running on all Manager Service hosts.

  d Verify that the last connected time for all IaaS Manager Service nodes is less than 30 seconds.

If you find any Management Agent connectivity issues, resolve them manually and retry the command to enable the Manager Service automatic failover.

- The manager-service-automatic-failover command fails to enable failover on a Manager Service node. It is safe to rerun the command to fix this.

- Some Manager Service hosts in the IaaS deployment have failover enabled while other hosts do not. All Manager Service hosts in the IaaS deployment must have the feature enabled or it does not work. To correct this issue, do one of the following:

  - Disable failover on all Manager Service nodes and use the manual failover approach instead.
    Only run failover on one host at a time.

  - If multiple attempts fail to enable the feature on a Manager Service node, stop the Windows VMware vCloud Automation Center Service on this node and set the node startup type to Manual until you resolve the issue.
Use Python to validate that failover is enabled on each Manager Service node.

- Log in to the master vRealize Automation appliance node as root using SSH.
- Verify that the system returns this message: Enabling Manager Service automatic failover mode on node: IAAS_MANAGER_SERVICE_NODEID done.

Validate that failover is enabled on each Manager Service node by inspecting the Manager Service configuration file.

- Open a command prompt on a Manager Service node.
- Navigate to the vRealize Automation installation folder and open the Manager Service configuration file at VMware\vCAC\Server\ManagerService.exe.config.
- Verify that the following elements are present in the <appSettings> section.
  - `<add key="FailoverModeEnabled" value="True" />`
  - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
  - `<add key="FailoverNodeState" value="active" />`
  - `<add key="FailoverMaxFailedDatabasePingAttepts" value="5" />`
  - `<add key="FailoverMaxFailedRepositoryPingAttepts" value="5" />`

- Verify that Windows VMware vCloud Automation Center Service status is started and startup type is automatic.

Use Python to validate that failover is disabled on each Manager Service node.

- Log in to the master vRealize Automation appliance node as root using SSH.
- Verify that the system returns this message: Disabling Manager Service automatic failover mode on node: IAAS_MANAGER_SERVICE_NODEID done.

Validate that failover is disabled on each Manager Service node by inspecting the Manager Service configuration file.

- Open a command prompt on a Manager Service node.
- Navigate to the vRealize Automation installation folder and open the Manager Service configuration file at VMware\vCAC\Server\ManagerService.exe.config.
- Verify that the following element is present in the <appSettings> section.
  - `<add key="FailoverModeEnabled" value="False" />`

To create a cold standby Manager Service node, set the node Windows VMware vCloud Automation Center Service status to stopped and startup type to manual.
For an active Manager Service node, the node Windows VMware vCloud Automation Center Service status must be started and startup type must be automatic.

The manager-service-automatic-failover command uses the Manager Service node internal id - IAAS_MANAGER_SERVICE_NODEID. To find the hostname corresponding to this internal id, run the command vra-command list-nodes and look for the Manager Service host with Nodeld: IAAS_MANAGER_SERVICE_NODEID.

To locate the Manager Service that the system has automatically elected to be currently active, perform these steps.

a Log in to the master vRealize Automation appliance node as root using SSH.

b Run vra-command list-nodes --components.

- If failover is enabled, find the Manager Service node with State: Active.
- If failover is disabled, find the Manager Service node with State: Started.

**Installation or Upgrade Fails with a Load Balancer Timeout Error**

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

**Problem**

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.

**Cause**

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

**Solution**

1. Increase your load balancer timeout value to at least 100 seconds.
2. Rerun the installation or upgrade.

**Upgrade Fails for IaaS Website Component**

The IaaS upgrade fails and you cannot continue the upgrade.

**Problem**

The IaaS upgrade fails for the website component. The following error messages appear in the installer log file.

- System.Data.Services.Client.DataServiceQueryException:
  
  An error occurred while processing this request. --->


- b Description: </b> An application error occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

- Done Building Project "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"
  (InstallRepoModel target(s)) -- FAILED.

The following error messages appear in the repository log file.

- [Error]: [sub-thread-Id="20"
  context="" token="""] Failed to start repository service. Reason: System.InvalidOperationException: Configuration section encryptionKey is not protected
  at DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration config)
  at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
  at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
  at
at DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String coreModelConnectionString)

**Cause**
IaaS upgrade fails when the creation date for the web.config file is the same as or later than the modified date.

**Solution**
1. On the IaaS host, log in to Windows.
2. Open the Windows command prompt.
3. Change directories to the vRealize Automation installation folder.
4. Start your preferred text editor with the **Run as Administrator** option.
5. Locate and select the web.config file and save the file to change its file modification date.
6. Examine the web.config file properties to confirm that the file modification date is later than the creation date.
7. Upgrade IaaS.

**Manager Service Fails to Run Due to SSL Validation Errors During Runtime**
The manager service fails to run due to SSL validation errors.

**Problem**
The manager service fails with the following error message in the log:

```
[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core database, will retry in 00:00:05, error details: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)
```

**Cause**
During runtime, the manager service fails to run due to SSL validation errors.

**Solution**
1. Open the ManagerService.config configuration file.
2 Update `Encrypt=False` on the following line:

```xml
<add name="vcac-repository" providerName="System.Data.SqlClient"
    connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
    Security=True;Pooling=True;Max Pool
    Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />```

### Log In Fails After Upgrade

You must exit the browser and log in again after an upgrade for sessions that use unsynchronized user accounts.

**Problem**

After you upgrade vRealize Automation, the system denies access to unsynchronized user accounts at login.

**Solution**

Exit the browser and relaunch vRealize Automation.

### Delete Orphaned Nodes on vRealize Automation

An orphaned node is a duplicate node that is reported on the host but does not exist on the host.

**Problem**

When you verify that each IaaS and virtual appliance node is in a healthy state, you might discover that a host has one or more orphaned nodes. You must delete all orphaned nodes.

**Solution**

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as `root` using the password you entered when you deployed the vRealize Automation appliance.

2. Select `vRA settings > Cluster`.

3. For each orphaned node in the table, click `Delete`.

### Join Cluster Command Appears to Fail After Upgrading a High-Availability Environment

After you click `Join Cluster` in the management console on a secondary cluster node, the progress indicator disappears.

**Problem**

When you use the vRealize Automation appliance management console after upgrade to join a secondary cluster node to the primary node, the progress indicator disappears and no error or success message appears. This behavior is an intermittent problem.
Cause

The progress indicator disappears because some browsers stop waiting for a response from the server. This behavior does not stop the join cluster process. You can confirm that the join cluster process is successful by viewing the log file at /var/log/vmware/vcac/vcac-config.log.

PostgreSQL Database Upgrade Merge Does Not Succeed

The external PostgreSQL database merge with the embedded PostgreSQL database does not succeed.

Problem

If the PostgreSQL database upgrade merge does not succeed, you can perform a manual merge.

Solution

1. Revert the vRealize Automation virtual appliance to the snapshot you made before upgrade.
2. Log in to the vRealize Automation virtual appliance and run this command to allow upgrade to complete if the database merge does not succeed.

   
   touch /tmp/allow-external-db
   
   The command does not disable auto merge.
3. On the remote PostgreSQL database host, connect to the PostgreSQL database using the psql tool and run these commands.

   CREATE EXTENSION IF NOT EXISTS "hstore";

   CREATE EXTENSION IF NOT EXISTS "uuid-ossp";

   CREATE SCHEMA saas AUTHORIZATION vcac;

   The user in this command is vcac. If vRealize Automation connects to the external database with a different user, replace vcac in this command with the name of that user.

   CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;

4. Run upgrade.

   If upgrade is successful, the system works as expected with the external PostgreSQL database. Ensure that the external PostgreSQL database is running properly.
5. Log in to the vRealize Automation virtual appliance and run these commands

   /etc/bootstrap/postupdate.d/00-20-db-merge-external

   /etc/bootstrap/postupdate.d/11-db-merge-external
Replica vRealize Automation Appliance Fails to Update

Replica vRealize Automation appliance fails to update during master appliance update.

Cause

A replica appliance can fail to update due to connectivity issues or other failures. When this happens, you see a warning message on the master vRealize Automation appliance Update tab, highlighting the replica that failed to update.

Solution

1. Revert the replica virtual appliance snapshot or backup to the pre-update state and power it on.
2. Log in as root to the replica vRealize Automation appliance management interface.
   
   https://vrealize-automation-appliance-FQDN:5480
3. Click Update > Settings.
4. Select to download the updates from a VMware repository or CDROM in the Update Repository section.
5. Click Status.
6. Click Check Updates to verify that an update is accessible.
7. Click Install Updates.
8. Click OK.

A message stating that the update is in progress appears.
9. Open the log files to verify that upgrade is progressing successfully.
   
   /opt/vmware/var/log/vami/vami.log
   /var/log/vmware/horizon/horizon.log

If you log out during the upgrade process and log in again before the upgrade is finished, you can continue to follow the progress of the update in the log file. The updatecli.log file might display information about the version of vRealize Automation that you are upgrading from. This displayed version changes to the proper version later in the upgrade process.

The time required for the update to finish varies according to your environment.
10. When the update is finished reboot the virtual appliance.
    
    a. Click System.
    
    b. Click Reboot and confirm your selection.
11. Select vRA Settings > Cluster.
12. Enter the master vRealize Automation appliance FQDN and click Join Cluster.
Backup Copies of .xml Files Cause the System to Time Out

vRealize Automation registers any file with an .xml extension in the \VMware\vCAC\Server\ExternalWorkflows\xml\db\ directory. If this directory contains backup files with an .xml extension, the system runs duplicate workflows that cause the system to time out.

Solution

Workaround: When you back up files in this directory, move the backups to another directory, or change the extension of the backup file name to something other than .xml.

Exclude IaaS Upgrade

You can update the vRealize Automation appliance without upgrading the IaaS components.

Use this procedure when you want to update the vRealize Automation appliance without upgrading the IaaS components. This procedure

- Does not stop IaaS services.
- Skips updating the Management Agents.
- Prevents the automatic update of IaaS components after the vRealize Automation appliance updates.

Procedure

1. Open a secure shell connection to the primary vRealize Automation appliance node.
2. At the command prompt, run this command to create the toggle file:
   ```bash
   touch /tmp/disable-iaas-upgrade
   ```
3. Manually stop the IaaS services.
   a. Log in to your IaaS Windows server.
   b. Select Start > Administrative Tools > Services.
   c. Stop these services in the following order.
      
      **Note**  Do not shut down the IaaS Windows server.
      
      1. Each VMware vRealize Automation Proxy Agent.
      2. Each VMware DEM worker.
      3. The VMware DEM orchestrator.
      4. The VMware vCloud Automation Center service.
4. Access the primary vRealize Automation appliance management console and update the primary vRealize Automation appliance.

Unable to Create New Directory in vRealize Automation

Trying to add new directory with the first sync connector fails.
Problem

This issue occurs due to a bad config-state.json file located in /usr/local/horizon/conf/states/VSPEHERE.LOCAL/3001/.

For information about fixing this issue, see Knowledge Base Article 2145438.

vRealize Automation Replica Virtual Appliance Update Times Out

vRealize Automation replica virtual appliance update times out when you update the master virtual appliance.

Problem

When you update the master virtual appliance, the master vRealize Automation management console update tab shows a highlighted replica virtual appliance that has reached the update timeout limit.

Cause

The update times out because of a performance or infrastructure issue.

Solution

1. Check the replica virtual appliance update progress.
   a. Go to the management console for your replica virtual appliance by using its fully qualified domain name (FQDN), https://va-hostname.domain.name:5480.
   b. Log in with the username root and the password you entered when the appliance was deployed.
   c. Select Update > Status and check the update progress.
      Do one of the following.
      - If the update fails, follow the steps in the troubleshooting topic Replica vRealize Automation Appliance Fails to Update.
      - If the replica virtual appliance upgrade is in progress, wait until the upgrade finishes and go to step 2.

2. Reboot the virtual appliance.
   a. Click System.
   b. Click Reboot and confirm your selection.

3. Select vRA Settings > Cluster.

4. Enter the master vRealize Automation virtual appliance FQDN, and click Join Cluster.

Some Virtual Machines Do Not Have a Deployment Created During Upgrade

Virtual machines in the missing state at the time of upgrade do not have a corresponding deployment created in the target environment.
Problem

If a virtual machine is in the missing state in the source environment during upgrade, a corresponding deployment is not created in the target environment. If a virtual machine goes out of the missing state after upgrade, you can import the machine to the target deployment using bulk import.

Certificate Not Trusted Error

When you view the infrastructure Log Viewer page in the vRealize Automation appliance console, you might see an endpoint connection failure report with these words, Certificate is not trusted.

Problem

On the vRealize Automation appliance console, select Infrastructure > Monitoring > Log. On the Log Viewer page, you might see a report similar to this:

Failed to connect to the endpoint. To validate that a secure connection can be established to this endpoint, go to the vSphere endpoint on the Endpoints page and click the Test Connection button.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Cause

Upgrading from vRealize Automation 7.3 or earlier to 7.4 makes changes to the endpoints from your original environment. For environments recently upgraded to vRealize Automation 7.4, the IaaS administrator must review each existing endpoint that uses a secure, https, connection. If an endpoint has a Certificate is not trusted error, the endpoint does not work properly.

Solution

1. Log in to the vRealize Automation console as an infrastructure administrator.
2. Select Infrastructure > Endpoints > Endpoints.
3. Complete these steps for each endpoint with a secure connection.
   a. Click Edit.
   b. Click Test Connection.
   c. Review the certificate details and click OK if you trust this certificate.
   d. Restart the Windows services for all IaaS Proxy Agents used by this endpoint.
4. Verify that Certificate is not trusted errors no longer appear on the infrastructure Log Viewer page.

Installation of Upgrade of vRealize Automation Fails While Applying Prerequisite Fixes

Installing or upgrading vRealize Automation fails and an error message appears in the log file.
Problem
When you install or upgrade vRealize Automation, the procedure fails. This usually happens when a fix applied during install or upgrade is not successful. An error message appears in the log file similar to the following: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Cause
The Windows environment has a group policy for PowerShell script execution set to Enabled.

Solution
1. On the Windows host machine, run gpedit.msc to open the Local Group Policy Editor.
2. In the left pane under Computer Configuration, click the expand button to open Administrative Templates > Windows Components > Windows PowerShell.
3. For Turn on Script Execution, change the state from Enabled to Not Configured.

Unable to Update DEM and DEO Components
Unable to update DEM and DEO components while upgrading from vRealize Automation 7.2 to 7.3.x

Problem
After upgrading from vRealize Automation 7.2 to 7.3.x, DEM and DEO components installed on custom path, such as D: drive, are not updated.

See Knowledge Base article 2150517.

Update Fails to Upgrade the Management Agent
An error message about the Management Agent appears when you click Install Updates on the vRealize Automation appliance management console Update Status page.

Problem
Upgrade process is unsuccessful. Message appears: Unable to upgrade management agent on node x. Sometimes the message lists more than one node.

Cause
Many conditions can cause this problem. The error message identifies only the node ID of the affected machine. More information is found in the All.log file for the Management Agent on the machine where the command fails.

Perform these tasks on the affected nodes according to your situation:

Solution
- If the Management Agent service is not running, start the service and restart upgrade on the virtual appliance.
If the Management Agent service is running and the Management Agent is upgraded, restart upgrade on the virtual appliance.

If the Management Agent service is running, but the Management Agent is not upgraded, perform a manual upgrade.

- Open a browser and navigate to the vRealize Automation IaaS installation page on the vRealize Automation appliance at https://va-hostname.domain.name:5480/install.
- Download and run the Management Agent Installer.
- Reboot the Management Agent machine.
- Restart upgrade on the virtual appliance.

Management Agent Upgrade is Unsuccessful

The Management Agent upgrade is unsuccessful while upgrading from vRealize Automation to 7.2 - 7.3.x.

Problem

If a failover incident has switched the primary and secondary Management Agent host, the upgrade is unsuccessful because the automated upgrade process cannot find the expected host. Perform this procedure on each IaaS node where the Management Agent is not upgraded.

Solution

1. Open the All.log in the Management Agent logs folder, which is located at C:\Program Files (x86)\VMware\vCAC\Management Agent\Logs\. The location of the installation folder might be different from the default location.

2. Search the log file for a message about an outdated or powered off virtual appliance.

   For example, INNER EXCEPTION: System.Net.WebException: Unable to connect to the remote server ----> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond IP_Address:5480

3. Edit the Management Agent configuration file at C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config to replace the existing alternativeEndpointaddress value with the URL of the primary virtual appliance endpoint.

   The location of the installation folder might be different from the default location.

   Example of alternativeEndpointaddress in VMware.IaaS.Management.Agent.exe.config.

   <alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />

4. Restart the Management Agent Windows service and check the All.log file to verify that it is working.
5 Run the upgrade procedure on the primary vRealize Automation appliance.

vRealize Automation Update Fails Because of Default Timeout Settings

You can increase the time setting for update if the default setting for synchronising databases is too short for your environment.

Problem

The timeout setting for the Vcac-Config SynchronizeDatabases command is not sufficient for some environments where synchronising databases takes longer than the default value of 3600 seconds.

The cafeTimeoutInSeconds and cafeRequestPageSize property values in the Vcac-Config.exe.config file govern the communication between the API and the Vcac-config.exe utility tool. The file is at IaaS installation location\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config.

You can override the default timeout value just for the SynchronizeDatabases command by supplying a value for these optional parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Short Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--DatabaseSyncTimeout</td>
<td>-dstm</td>
<td>Sets the http request timeout value only for SynchronizeDatabases in seconds.</td>
</tr>
<tr>
<td>--DatabaseSyncPageSize</td>
<td>-dsps</td>
<td>Sets the sync request page size only for Reservation or Reservation Policy synchronization. The default is 10.</td>
</tr>
</tbody>
</table>

If these parameters are not set in the Vcac-Config.exe.config file, the system uses the default timeout value.

Upgrading IaaS in a High Availability Environment Fails

Running the IaaS upgrade process on the primary web server node with load balancing enabled fails. You might see these error messages: "System.Net.WebException: The operation has timed out" or "401 - Unauthorized: Access is denied due to invalid credentials."

Problem

Upgrading IaaS with load balancing enabled can cause an intermittent failure. When this happens, you must run the vRealize Automation upgrade again with load balancing disabled.

Solution

1 Revert your environment to the pre-update snapshots.
2 Open a remote desktop connection to the primary IaaS web server node.
3 Navigate to the Windows hosts file at c:\windows\system32\drivers\etc.
4. Open the hosts file and add this line to bypass the web server load balancer:

```
IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn
```

Example:

```
10.10.10.5 vra-iaas-web-lb.domain.com
```

5. Save the hosts file and retry the vRealize Automation update.

6. When the vRealize Automation update competes, open the hosts file and remove the line you added in step 4.

**Work Around Upgrade Problems**

You can modify the upgrade process to work around upgrade problems.

**Solution**

When you experience problems upgrading your vRealize Automation environment, use this procedure to modify the upgrade process by selecting one of the available flags.

**Procedure**

1. Open a secure shell connection to the primary vRealize Automation appliance node.

2. At the command prompt, run this command to create the toggle file:

```
touch available_flag
```

For example: `touch /tmp/disable-iaas-upgrade`

**Table 1-77. Available Flags**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/disable-iaas-upgrade</td>
<td>- Prevents IaaS upgrade process after the virtual appliance restarts.</td>
</tr>
<tr>
<td></td>
<td>- Prevents the Management Agent upgrade.</td>
</tr>
<tr>
<td></td>
<td>- Prevents the automatic prerequisite checks and fixes.</td>
</tr>
<tr>
<td></td>
<td>- Prevents stopping IaaS services.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-ma</td>
<td>Prevents the Management Agent upgrade. This flag is suitable when the Management Agent is upgraded manually.</td>
</tr>
<tr>
<td>/tmp/skip-prreq-checks</td>
<td>Prevents the automatic prerequisite checks and fixes.</td>
</tr>
<tr>
<td></td>
<td>This flag is suitable when there is a problem with the automatic prerequisite fixes and the fixes have been applied manually instead.</td>
</tr>
<tr>
<td>/tmp/do-not-stop-services</td>
<td>Prevents stopping IaaS services. The upgrade does not stop the IaaS Windows services, such as the Manager Service, DEMs, and agents.</td>
</tr>
</tbody>
</table>
### Table 1-77. Available Flags (Continued)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/do-not-upgrade-servers</td>
<td>Prevents the automatic upgrade of all server IaaS components, such as the database, web site, WAPI, repository, Model Mfrontanager data, and Manager Service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This flag also prevents enabling the Manager Service automatic failover mode.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-dems</td>
<td>Prevents DEM upgrade.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-agents</td>
<td>Prevents IaaS proxy agent upgrade.</td>
</tr>
</tbody>
</table>

3 Complete the tasks for your chosen flag.

### Table 1-78. Additional Tasks

<table>
<thead>
<tr>
<th>Flag</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/disable-iaas-upgrade</td>
<td>■ Upgrade the Management Agent manually.</td>
</tr>
<tr>
<td></td>
<td>■ Apply any required IaaS prerequisites manually.</td>
</tr>
<tr>
<td></td>
<td>■ Manually stop the IaaS services.</td>
</tr>
<tr>
<td></td>
<td>a Log in to your IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>b Select <strong>Start &gt; Administrative Tools &gt; Services</strong>.</td>
</tr>
<tr>
<td></td>
<td>c Stop these services in the following order.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not shut down the IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>a Each VMware vRealize Automation Proxy Agent.</td>
</tr>
<tr>
<td></td>
<td>b Each VMware DEM worker.</td>
</tr>
<tr>
<td></td>
<td>c The VMware DEM orchestrator.</td>
</tr>
<tr>
<td></td>
<td>d The VMware vCloud Automation Center service.</td>
</tr>
<tr>
<td></td>
<td>■ Start the IaaS upgrade manually after the virtual appliance upgrade is complete.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-ma</td>
<td>Upgrade the Management Agent manually.</td>
</tr>
<tr>
<td>/tmp/skip-prereq-checks</td>
<td>Apply any required IaaS prerequisites manually.</td>
</tr>
<tr>
<td>/tmp/do-not-stop-services</td>
<td>Manually stop the IaaS services.</td>
</tr>
<tr>
<td></td>
<td>1 Log in to your IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>2 Select <strong>Start &gt; Administrative Tools &gt; Services</strong>.</td>
</tr>
<tr>
<td></td>
<td>3 Stop these services in the following order.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not shut down the IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>a Each VMware vRealize Automation Proxy Agent.</td>
</tr>
<tr>
<td></td>
<td>b Each VMware DEM worker.</td>
</tr>
<tr>
<td></td>
<td>c The VMware DEM orchestrator.</td>
</tr>
<tr>
<td></td>
<td>d The VMware vCloud Automation Center service.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-servers</td>
<td>Prevents the automatic upgrade of all server IaaS components, such as the database, web site, WAPI, repository, Mfrontanager data, and Manager Service.</td>
</tr>
</tbody>
</table>

**Note** This flag also prevents enabling the Manager Service automatic failover mode.
Table 1-78. Additional Tasks (Continued)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/do-not-upgrade-dems</td>
<td></td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-agents</td>
<td></td>
</tr>
</tbody>
</table>

4 Access the primary vRealize Automation appliance management console and update the primary vRealize Automation appliance.

**Note** Because each flag remains active until it is removed, run this command to remove your chosen flag after upgrade: `rm /flag_path/flag_name`. For example, `rm /tmp/disable-iaas-upgrade`.

**Virtual Appliance Upgrade Fails During the IaaS Prerequisite Check**

IaaS prerequisite check is unable to validate environments configured with a custom IIS website name. Disabling the automated IaaS upgrade corrects the problem.

**Problem**

The virtual appliance upgrade fails during the IaaS prerequisite check while running pre-install scripts and post-install scripts.

**Error:** Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

When the failure occurs, you see an error message similar to: Applying automatic fix for `<prerequisite check name>` prerequisite failed.

**Cause**

IaaS prerequisite check is unable to validate environments configured with a custom IIS website name. Disabling the automated IaaS upgrade prerequisite checks corrects the problem.

**Solution**

1 Disable the automated IaaS upgrade prerequisite checks and fixes.

2 Run the vRealize Automation upgrade. See Work Around Upgrade Problems.

3 Follow the upgrade prompts. When the prompts direct you to reboot vRealize Automation, you can use the IaaS installer to search for any unsatisfied IaaS prerequisites and fix them manually.

**Note** Do not restart the appliance until you finish the IaaS prerequisites validation.

4 Use the following steps for every IaaS website node.

   a Download the IaaS installer. See Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance.

   b The first time you initialize the IaaS installer, it generates a new configuration file under the same directory with extension .exe.config.
c Close the IaaS installer and add the following key in the <appSettings> section of the configuration file. The key passes your custom website name to the IaaS prerequisite checker.

```xml
<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>
```

d Save the configuration file and rerun the IaaS Installer. Follow the onscreen instructions, until the prerequisite validation is finished. If there were any failed prerequisites, fix them manually.

5 Activate the IaaS automatic upgrade by closing the IaaS installer and rebooting the upgraded vRealize Automation appliance.

**Note** If you decide to continue the IaaS upgrade manually using the IaaS Installer, first reboot the upgraded vRealize Automation appliance, wait for all services to become registered. You must upgrade and configure all systems that have IaaS components installed. For more information, see Upgrade the IaaS Components After Upgrading vRealize Automation 7.1 or 7.2 to 7.3.

### Upgrading vRealize Automation 6.2.5 to 7.4

When you upgrade your vRealize Automation 6.2.5 environment to the latest version, you use upgrade procedures specific to your 6.2.5 environment.

This information is specific to upgrading vRealize Automation 6.2.5 to 7.4. For information about other supported upgrade paths, see Upgrading vRealize Automation.

### Upgrading vRealize Automation 6.2.5 to 7.4

You can perform an in-place upgrade of your current vRealize Automation 6.2.5 environment to 7.4. You use upgrade procedures specific to this version to upgrade your environment.

An in-place upgrade is a three-stage process. You update the components in your current environment in this order.

1 vRealize Automation appliance
2 IaaS web server
3 vRealize Orchestrator

You must upgrade all product components to the same version.

The vRealize Production Test Upgrade Assist Tool analyzes your vRealize Automation 6.2.x environment for any feature configuration that can cause upgrade issues and checks that your environment is ready for upgrade. To download this tool and related documentation, go to the VMware vRealize Production Test Tool download product page.

Property dictionary controls that are not supported after upgrade can be restored using vRealize Orchestrator and property dictionary relationships.

If you have workflows in your source environment that contain deprecated code, see the vRealize Automation Extensibility Migration Guide for information about the code changes required for conversion to event broker subscriptions.
Beginning with vRealize Automation 7.2, JFrog Artifactory Pro is no longer bundled with the vRealize Automation appliance. If you upgrade from an earlier version of vRealize Automation, the upgrade process removes JFrog Artifactory Pro. For more information, see Knowledge Base 2147237.

**Note**  If you have customized your current vRealize Automation 6.2.5 environment, contact your CCE support staff for additional upgrade information.

Prerequisites for Upgrading vRealize Automation

Before you upgrade from vRealize Automation 6.2.5, review the following prerequisites.

**System Configuration Requirements**

Verify that the following system requirements are met before you begin an upgrade.

- Verify that all appliances and servers that are part of your deployment meet the system requirements for the latest version. See the [vRealize Automation Support Matrix](https://www.vmware.com/support/vrealize documentation) at VMware vRealize Automation Documentation.

- Consult the [VMware Product Interoperability Matrix](https://www.vmware.com/support/vmware_products.html) on the VMware website for information about compatibility with other VMware products.

- Verify that the vRealize Automation you are upgrading from is in stable working condition. Correct any problems before upgrading.

- If you are upgrading from vRealize Automation 6.2.5, record the vCloud Suite license key you use for your current vRealize Automation environment. Upon upgrade, existing license keys are removed from the database.

- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.

**Hardware Configuration Requirements**

Verify that the hardware in your environment is adequate for vRealize Automation your target release. See [vRealize Automation Hardware Specifications and Capacity Maximums](https://www.vmware.com/support/vrealize documentation)

Verify that the following system requirements are met before you begin an upgrade.

- You must configure your current hardware before you download the upgrade. See [Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5](https://www.vmware.com/support/vmware_products.html).

- You must have at least 18 GB RAM, 4 CPUs, Disk1=50 GB, Disk3=25 GB, and Disk4=50 GB before you run the upgrade.

  If the virtual machine is on vCloud Networking and Security, you might need to allocate more RAM space.

  Although general support for vCloud Networking and Security has ended, the VCNS custom properties continue to be valid for NSX purposes. See the Knowledge Base article [2144733](https://www.vmware.com/support/kb article.html).

- These nodes must have at least 5 GB of free disk space:
  - Primary IaaS Website
Microsoft SQL database

Model Manager

The primary IaaS Website node where the Model Manager data is installed must have JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, you must set the JAVA_HOME environment variable to the new version.

To download and run the upgrade, you must have the following resources:

- At least 5 GB on the root partition
- 5 GB on the /storage/db partition for the master vRealize Automation appliance
- 5 GB on the root partition for each replica virtual appliance
- Check the /storage/log subfolder and remove any older archived ZIP files to clean up space.

General Prerequisites

Verify that the following system requirements are met before you begin an upgrade.

- You have access to an Active Directory account with a username@domain format and permissions to bind to the directory.
- You meet these conditions:
  - You have access to an account with a SAMaccountName format.
  - You have sufficient privileges to join the system to the domain by creating a computer object dynamically or to merge into a pre-created object.
- You have access to all databases and all load balancers impacted by or participating in the vRealize Automation upgrade.
- You make the system unavailable to users while you perform the upgrade.
- You disable any applications that query vRealize Automation.
- Verify that Microsoft Distributed Transaction Coordinator (MSDTC) is enabled on all vRealize Automation and associated SQL servers. For instructions, see Knowledge Base article 2089503.
- If your environment has an external vRealize Orchestrator appliance, and an external vRealize Orchestrator appliance connected to the Identity Appliance, upgrade vRealize Orchestrator before you upgrade vRealize Automation.
- You must complete additional tasks to prepare your vRealize Automation virtual machines before you upgrade. Before you upgrade, review Knowledge Base article 51531.
- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.
- If you use the DynamicTypes plugin, export the vRealize Orchestrator DynamicTypes plug-in configuration as a package.
  - Log in to the Java Client as an administrator user.
b Select the **Workflows** tab.

c Select **Library > Dynamic Types > Configuration**.

d Select the Export Configuration as Package workflow and run it.

e Click **Not Set > Insert value**.

f Select the namespaces you want to export and click **Add** to add them to the package.

g Click **Submit** to export the package.

- Complete these steps if you are upgrading a distributed environment configured with an embedded PostgreSQL database.

  a Examine the files in the **pgdata** directory on the master host before you upgrade the replica hosts.

  b Navigate to the PostgreSQL data folder on the master host at `/var/vmware/vpostgres/current/pgdata/`.

  c Close any opened files in the **pgdata** directory and remove any files with a `.swp` suffix.

  d Verify that all files in this directory have correct ownership: `postgres:users`.

**Considerations About Upgrading to This vRealize Automation Version**

vRealize Automation 7 and later introduces various functional changes during and after the upgrade process. You should review changes before you upgrade your vRealize Automation 6.2.5 deployment to the new version.

Review these considerations before you upgrade.

**Upgrade and Identity Appliance Specifications**

During the vRealize Automation upgrade process, you answer prompts to upgrade the identity appliance.

The target deployment uses the VMware Identity Manager.

**Upgrade and Licensing**

During the upgrade, your existing vRealize Automation 6.2.5 licenses, and any vCloud Suite 6.x licenses that you have, are removed. You must reenter your licenses in the vRealize Automation 7.4 vRealize Automation appliance management console.

You now use vRealize Automation licensing for virtual appliances and IaaS by entering license key information in the vRealize Automation appliance. Licensing information is no longer available in the IaaS user interface and IaaS no longer performs licensing checks. Endpoints and quotas are enforced through the end-user license agreements (EULAs).

**Note** Write down your vCloud Suite 6.x license key if you used it for vRealize Automation 6.2.5 before the upgrade. Upon upgrade, existing license keys are removed from the database.

For more information about reentering your license information during or after upgrade, see **Update the License Key**.
Understanding How Roles Are Upgraded

When you upgrade vRealize Automation, your organization's existing role assignments are maintained. The upgrade also creates some role assignments to support additional blueprint architect roles.

The following architect roles are used to support the blueprint definition in the design canvas:

- Application architect. Assembles existing components and blueprints to create composite blueprints.
- Infrastructure architect. Creates and manages virtual machine blueprints.
- XaaS architect. Creates and manages XaaS blueprints.
- Software architect. Creates and manages Software components.

In vRealize Automation 7, tenant administrators and business group managers cannot design blueprints by default. Upgraded tenant administrators and business group managers are given the infrastructure architect role.

Users who can reconfigure a virtual machine in the vRealize Automation 6.2.x source version can change virtual machine ownership after you upgrade to the new version.

The following role assignments are made during the upgrade. Roles that are not listed in the table are upgraded to the same role name in the target deployment.

<table>
<thead>
<tr>
<th>Role in Source Deployment</th>
<th>Role in Target Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant administrator</td>
<td>Tenant administrator and Infrastructure architect</td>
</tr>
<tr>
<td>Business group manager</td>
<td>Business group manager and Infrastructure architect</td>
</tr>
<tr>
<td>Service architect</td>
<td>XaaS architect</td>
</tr>
<tr>
<td>Application architect</td>
<td>Software architect</td>
</tr>
</tbody>
</table>

For more information about roles, see Tenant Roles and Responsibilities in vRealize Automation.

Understanding How Blueprints Are Upgraded

As a rule, published blueprints are upgraded as published blueprints.

However, there are exceptions to that rule. Multi-machine blueprints are upgraded as composite blueprints that contain blueprint components. Multi-machine blueprints that contain unsupported settings are upgraded as unpublished.

**Note** vRealize Automation 7.x takes a blueprint snapshot at deployment. If you encounter reconfigure problems when updating machine properties such as CPU and RAM in a deployment, see Knowledge Base article 2150829 vRA 7.x Blueprint Snapshotting.

For more information about upgrading blueprints, see Upgrade and vApp Blueprints, vCloud Endpoints, and vCloud Reservations and Understanding How Multi-Machine Blueprints Are Upgraded.
Upgrade and vApp Blueprints, vCloud Endpoints, and vCloud Reservations

You cannot upgrade a deployment that contains vApp (vCloud) endpoints. The presence of vApp (vCloud) endpoints prevents upgrade to this vRealize Automation version.

Upgrade fails on the master virtual appliance if there is a vApp (vCloud) endpoint in the source deployment. A message appears in the user interface and log. To determine if your source deployment contains a vApp (vCloud) endpoint, log in to the vRealize Automation console as IaaS administrator user. Select *Infrastructure > Endpoints*. If the endpoints list contains vApp (vCloud) endpoints, you cannot upgrade to this vRealize Automation version.

Managed vApps for vCloud Air or vCloud Director resources are not supported in the target vRealize Automation environment.

**Note**  The following approval policy types are deprecated. If they appear in the list of available approval policy types after upgrade is finished, they are unusable.

- Service Catalog - Catalog Item Request - vApp
- Service Catalog - Catalog Item Request - vApp Component

You can create vCloud Air and vCloud Director endpoints and reservations in the target deployment. You can also create blueprints with vCloud Air or vCloud Director virtual machine components.

Understanding How Multi-Machine Blueprints Are Upgraded

You can upgrade managed service, multi-machine blueprints from a supported vRealize Automation 6.2.x version deployment.

When you upgrade a multi-machine blueprint, component blueprints are upgraded as separate single-machine blueprints. The multi-machine blueprint is upgraded as a composite blueprint in which its previous children blueprints are nested as separate blueprint components.

The upgrade creates a single composite blueprint in the target deployment that contains one virtual machine component for each component blueprint in the source multi-machine blueprint. If a blueprint has a setting that is not supported in the new version, the blueprint is upgraded and set to draft status. For example, if the multi-machine blueprint contains a private network profile, upgrade ignores the profile setting, and the blueprint is upgraded in a draft state. You can edit the draft blueprint to enter supported network profile information and publish it.

**Note**  If a published blueprint in the source deployment is upgraded to a draft status blueprint, the blueprint is no longer part of a service or entitlement. After you update and publish the blueprint in the upgraded vRealize Automation version, you must recreate its needed approval policies and entitlements.

Some multi-machine blueprint settings are not supported in the target vRealize Automation deployment, including private network profiles and routed network profiles with associated PLR edge settings. If you have used a custom property to specify PLR edge settings (VCNS.LoadBalancerEdgePool.Names), the custom property is upgraded.
You can upgrade a multi-machine blueprint with vSphere endpoints and NSX network and security settings. The upgraded blueprint contains NSX network and security components in the design canvas.

**Note** Routed gateway specifications for multi-machine blueprints, as defined in reservations, are upgraded. However, the target vRealize Automation deployment does not support reservations for routed profiles that contain associated PLR edge settings. If the source reservation contains a routed gateway value for a PLR edge, the reservation is upgraded but the routed gateway setting is ignored. As a result, the upgrade generates an error message in the log file and the reservation is disabled.

During upgrade, spaces and special characters are removed from referenced network and security component names.

**Note** vRealize Automation 7.x takes a blueprint snapshot at deployment. If you encounter reconfigure problems when updating machine properties such as CPU and RAM in a deployment, see Knowledge Base article 2150829 vRA 7.x Blueprint Snapshotting.

Depending on the setting type, the network and security information is captured as several different settings in the new blueprint.

- Settings for the overall blueprint on its properties page. This information includes app isolation, transport zone, and routed gateway or NSX edge reservation policy information.
- Available settings for vSphere virtual machine components in NSX network and security components in the design canvas.
- Settings in the network and security tabs of individual vSphere virtual machine components in the design canvas.

**Upgrade and Physical Endpoints, Reservations, and Blueprints**

You cannot upgrade a deployment that contains physical endpoints. If physical endpoints are present, the vRealize Automation upgrade process fails.

Upgrade fails on the master virtual appliance when the vRealize Automation 6.2.x deployment has a physical endpoint. A failure message appears in the migration interface and log. To determine if your vRealize Automation 6.2.x deployment has a physical endpoint, log in to vRealize Automation as an IaaS administrator user. Select **Infrastructure > Endpoints** and review the endpoints list. If the list has a **Platform Type Physical** endpoint, you cannot upgrade to vRealize Automation 7.0 and later.

Physical endpoints, reservations, and virtual machine components in blueprints are not supported in vRealize Automation 7.0 and later.

**Upgrade and Network Profile Settings**

Private network profiles are not supported in vRealize Automation 7 and later. These profiles are ignored during the upgrade. Routed network profiles with associated PLR edge settings are also not supported in vRealize Automation 7 and later. These profiles are also ignored during the upgrade.
The private network profile type is not supported in vRealize Automation 7 and later. When the vRealize Automation upgrade process finds a private network profile in the source deployment, it ignores the network profile. Load balancers that reference those private networks are also ignored during upgrade. The same upgrade conditions are true for a routed network profile with associated PLR edge settings. Neither network profile configuration is upgraded.

If a reservation contains a private network profile, the private network profile setting is ignored during upgrade. The reservation is upgraded as disabled in the target deployment.

If a reservation contains a routed network profile with associated PLR edge settings, the routed network profile specification is ignored during upgrade. The reservation is upgraded as disabled in the target deployment.

For information about upgrading a multi-machine blueprint that contains network settings, see Understanding How Multi-Machine Blueprints Are Upgraded.

Upgrade and Entitled Actions
You cannot upgrade virtual machine actions.

The actions that you can perform on provisioned virtual machines, based on blueprint specifications, are not upgraded. To recreate the actions you can perform on a virtual machine, customize the entitlements for blueprints to enable only certain actions.

For related information, see Actions in Entitlements.

Upgrade and Custom Properties
All the custom properties that vRealize Automation supplies are available in the upgraded deployment. Custom properties and property groups are upgraded.

Terminology and Related Changes
All the build profiles that you created in the source deployment are upgraded as property groups. The term build profile has been retired.

The term property set has been retired and CSV property set files are no longer available.

Case-sensitivity in Custom Property Names
Before vRealize Automation 7.0, custom property names were case-insensitive. In vRealize Automation 7.0 and later, custom property names are case-sensitive. During upgrade, custom property names must be an exact match. This ensures that property values do not override one another and that they match property dictionary definitions. For example, a custom property hostname and another custom property HOSTNAME are considered different custom properties by vRealize Automation 7.0 and later. The custom property hostname and the custom property HOSTNAME do not override one another during upgrade.
Spaces in Custom Property Names

Before upgrading to this release of vRealize Automation, remove any space characters from your custom property names, for example replace the space with an underscore character, to allow the custom property to be recognized in the upgraded vRealize Automation installation. vRealize Automation custom property names cannot contain spaces. This issue can also impact use of an upgraded vRealize Orchestrator installation that uses custom properties that contained spaces in earlier releases of either vRealize Automation or vRealize Orchestrator or both.

Reserved Property Names

Because several keywords are now reserved, some upgraded properties might be affected. Some keywords that are used by the blueprint code can be imported, for example, by using vRealize CloudClient blueprint import functions. These keywords are considered reserved and are not available for properties that are being upgraded. The keywords include but are not limited to cpu, storage, and memory.

Upgrade and Application Services

Application Services upgrade is supported in vRealize Automation 7 and later.

After successful migration to vRealize Automation 7.4, you can use the vRealize Automation Application Services Migration Tool to upgrade your application services. Complete these steps to download the tool.

1. Click Download VMware vRealize Automation.

2. Select Drivers & Tools > VMware vRealize Application Services Migration Tool.

Upgrade and Advanced Service Design

When you upgrade to vRealize Automation 7 and later, your Advanced Service Design items are upgraded to XaaS elements.

XaaS components are available for use in the design canvas.

Upgrade and Blueprint Price Information

As of 7.0, vRealize Automation price profiles are no longer supported and are not migrated into the target deployment during upgrade. However, you can use the enhanced integration with vRealize Business for Cloud to manage your vRealize Automation resource expenses.

vRealize Business for Cloud is now tightly integrated with vRealize Automation and supports the following enhanced pricing features.

- Unified location in vRealize Business for Cloud to define flexible pricing policies for:
  - Infrastructure resource, machine, and application blueprints
  - Provisioned virtual machines in vRealize Automation for supported endpoints such as vCenter Server, vCloud Director, Amazon Web Services, Azure, and OpenStack.
  - Any operational price, one time price, and price on custom properties of provisioned virtual machines
  - Deployments, which include the price of virtual machines within the deployments
- Role-based showback reports in vRealize Business for Cloud
- Fully leverage new features in vRealize Business for Cloud

Before you upgrade, you can export your existing expense reports from your source vRealize Automation instance for reference. After you finish your upgrade, you can install and configure vRealize Business for Cloud to handle pricing.

**Note**  vRealize Automation 7.4 is compatible only with vRealize Business for Cloud 7.4 and later.

### Upgrade and Catalog Items

After you upgrade from vRealize Automation 6.2.x to the latest version, some catalog items appear in the service catalog but are not available to request.

After you migrate to the latest version of vRealize Automation, catalog items that use these property definitions appear in the service catalog but are not available to request.

- Control types: Check box or link.
- Attributes: Relationship, regular expressions, or property layouts.

In vRealize Automation 7.x, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see [Catalog Items Appear in the Service Catalog After Upgrade But Are Not Available to Request](#).

### Checklist for Upgrading vRealize Automation

When you upgrade vRealize Automation from 6.2.5 to 7.4, you update all vRealize Automation components in a specific order.

Use the checklists to track your work as you complete the upgrade. Finish the tasks in the order they are given.

**Note**  You must upgrade components in the prescribed order and upgrade all components. Using a different order can result in an unexpected behavior after the upgrade or failure of the upgrade to complete.

The order of upgrade varies depending on whether you are upgrading a minimal environment or a distributed environment with multiple vRealize Automation appliances.
### Table 1-80. Checklist to Upgrade a Minimal vRealize Automation Environment

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up your current installation. Making this backup is a critical</td>
<td>For more information on how to back up and restore your system, see Back Up Your Existing vRealize Automation 6.2.5 Environment. For general information, see Configuring Backup and Restore by Using Symantec Netbackup at <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a></td>
</tr>
<tr>
<td>task.</td>
<td></td>
</tr>
<tr>
<td>Prepare vRealize Automation 6.2.x virtual machines for upgrade.</td>
<td>You must review Knowledge Base article 51531 and perform any relevant fixes to your environments prior to upgrade.</td>
</tr>
<tr>
<td>If the Common Components Catalog is installed, you must uninstall it</td>
<td>For information about how to uninstall Common Components Catalog components, see the Common Components Catalog Installation Guide. If this guide is unavailable, do these steps on each IaaS node.</td>
</tr>
<tr>
<td>before you upgrade.</td>
<td>1 Log in to the IaaS node.</td>
</tr>
<tr>
<td></td>
<td>2 Click Start.</td>
</tr>
<tr>
<td></td>
<td>3 Enter services in the Search programs and files text box.</td>
</tr>
<tr>
<td></td>
<td>4 Click Services.</td>
</tr>
<tr>
<td></td>
<td>5 In the right pane of the Services window, right-click each IaaS service and select Stop to stop each service.</td>
</tr>
<tr>
<td></td>
<td>6 Click Start &gt; Control Panel &gt; Programs and Features.</td>
</tr>
<tr>
<td></td>
<td>7 Right-click each installed Common Components Catalog component, and select Uninstall.</td>
</tr>
<tr>
<td></td>
<td>8 Click Start &gt; Command Prompt.</td>
</tr>
<tr>
<td></td>
<td>9 At the command prompt, run iisreset.</td>
</tr>
<tr>
<td>Review Considerations for Upgrading to this vRealize Automation</td>
<td>See Considerations About Upgrading to This vRealize Automation Version.</td>
</tr>
<tr>
<td>Version to know what can be upgraded, what cannot be upgraded, and</td>
<td></td>
</tr>
<tr>
<td>how upgraded items might behave differently.</td>
<td></td>
</tr>
<tr>
<td>Not all items, including blueprints, reservations, and endpoints</td>
<td></td>
</tr>
<tr>
<td>can be upgraded. The presence of some unsupported configurations</td>
<td></td>
</tr>
<tr>
<td>blocks upgrade.</td>
<td></td>
</tr>
<tr>
<td>Configure your hardware resources.</td>
<td>See Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5.</td>
</tr>
<tr>
<td>Download updates to the vRealize Automation appliance.</td>
<td>See Downloading vRealize Automation Appliance Updates.</td>
</tr>
<tr>
<td>Install the update on the vRealize Automation appliance.</td>
<td>See Install the Update on the vRealize Automation Appliance.</td>
</tr>
<tr>
<td>Update the Single-Sign On utility to the VMware Identity Manager</td>
<td>See Update Your Single Sign-On Password for VMware Identity Manager.</td>
</tr>
</tbody>
</table>
### Table 1-80. Checklist to Upgrade a Minimal vRealize Automation Environment (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update the license key.</td>
<td>See Update the License Key.</td>
</tr>
<tr>
<td>Migrate the Identity Store to the VMware Identity Manager</td>
<td></td>
</tr>
<tr>
<td>Upgrade IaaS components.</td>
<td>See Upgrading the IaaS Server Components After Upgrading vRealize Automation.</td>
</tr>
<tr>
<td>Upgrade the external vRealize Orchestrator.</td>
<td>See Upgrading Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation.</td>
</tr>
<tr>
<td>Add users or groups to an Active Directory connection.</td>
<td>See Add Users or Groups to an Active Directory Connection.</td>
</tr>
</tbody>
</table>

### Table 1-81. Checklist to Upgrade a vRealize Automation Distributed Environment

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up your current installation. Making this backup is a critical task.</td>
<td>For more information on how to back up and restore your system, see Back Up Your Existing vRealize Automation 6.2.5 Environment. For detailed information, see Configuring Backup and Restore by Using Symantec Netbackup at <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a></td>
</tr>
<tr>
<td>Prepare vRealize Automation 6.2.x virtual machines for upgrade.</td>
<td>You must review Knowledge Base article 51531 and perform any relevant fixes to your environments prior to upgrade.</td>
</tr>
</tbody>
</table>
| If the Common Components Catalog is installed, you must uninstall it before you upgrade. | For information about how to uninstall Common Components Catalog components, see the Common Components Catalog Installation Guide. If this guide is unavailable, do these steps on each IaaS node.  
1 Log in to the IaaS node.  
2 Click Start.  
3 Enter services in the Search programs and files text box.  
4 Click Services.  
5 In the right pane of the Services window, right-click each IaaS service and select Stop to stop each service.  
6 Click Start > Control Panel > Programs and Features.  
7 Right-click each installed Common Components Catalog component, and select Uninstall.  
8 Click Start > Command Prompt.  
9 At the command prompt, run iisreset. |
Table 1-81. Checklist to Upgrade a vRealize Automation Distributed Environment (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure your hardware resources for the upgrade.</td>
<td>See Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5.</td>
</tr>
<tr>
<td>2. Disable your load balancers.</td>
<td>Disable each secondary node and remove the vRealize Automation health monitors for the following items.  ■ vRealize Automation appliance  ■ IaaS website  ■ IaaS Manager Service  For a successful upgrade, verify the following:  ■ Load balancer traffic is directed only to the primary node.  ■ vRealize Automation health monitors are removed for the appliance, website, and Manager Service.</td>
</tr>
<tr>
<td>3. Download updates to the vRealize Automation appliance.</td>
<td>See Downloading vRealize Automation Appliance Updates.</td>
</tr>
<tr>
<td>4. Install the update on the first vRealize Automation appliance in your installation. If you have designated an appliance as a master, upgrade this appliance first.</td>
<td>See Install the Update on the vRealize Automation Appliance.</td>
</tr>
<tr>
<td>5. Update the Single-Sign On utility to the VMware Identity Manager utility.</td>
<td>See Update Your Single Sign-On Password for VMware Identity Manager.</td>
</tr>
<tr>
<td>6. Update the license key.</td>
<td>See Update the License Key.</td>
</tr>
<tr>
<td>7. Migrate the Identity Store to the VMware Identity Manager utility.</td>
<td>Migrate Identity Stores to VMware Identity Manager</td>
</tr>
<tr>
<td>8. Install the update on the rest of your vRealize Automation appliances.</td>
<td>Install the Update on Additional vRealize Automation Appliances</td>
</tr>
<tr>
<td>10. Upgrade the external vRealize Orchestrator.</td>
<td>See Upgrading Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation.  See Upgrading External vRealize Orchestrator Appliance Cluster for Use with vRealize Automation</td>
</tr>
<tr>
<td>11. Enable your load balancers.</td>
<td>Enable Your Load Balancers</td>
</tr>
</tbody>
</table>

vRealize Automation Environment User Interfaces

You use and manage your vRealize Automation environment with several interfaces.

User Interfaces

These tables describe the interfaces that you use to manage your vRealize Automation environment.
Table 1-82. vRealize Automation Administration Console

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Automation console for these system administrator tasks.</td>
<td>1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
</tr>
<tr>
<td>■ Add tenants.</td>
<td>2 Click vRealize Automation console.</td>
</tr>
<tr>
<td>■ Customize the vRealize Automation user interface.</td>
<td>You can also use this URL to open the vRealize Automation console: <a href="https://vra-va-hostname.domain.name/vcac">https://vra-va-hostname.domain.name/vcac</a></td>
</tr>
<tr>
<td>■ Configure email servers.</td>
<td>3 Log in.</td>
</tr>
<tr>
<td>■ View event logs.</td>
<td></td>
</tr>
<tr>
<td>■ Configure vRealize Orchestrator.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must be a user with the system administrator role.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-83. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use vRealize Automation for these tasks.</td>
<td>1 Start a browser and enter the URL of your tenancy using the fully qualified domain name of the virtual appliance and the tenant URL name: <a href="https://vra-va-hostname.domain.name/vcac.org/tenant_URL_name">https://vra-va-hostname.domain.name/vcac.org/tenant_URL_name</a> .</td>
</tr>
<tr>
<td>■ Request new IT service blueprints.</td>
<td>2 Log in.</td>
</tr>
<tr>
<td>■ Create and manage cloud and IT resources.</td>
<td></td>
</tr>
<tr>
<td>■ Create and manage custom groups.</td>
<td></td>
</tr>
<tr>
<td>■ Create and manage business groups.</td>
<td></td>
</tr>
<tr>
<td>■ Assign roles to users.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must be a user with one or more of these roles:</td>
<td></td>
</tr>
<tr>
<td>■ Application Architect</td>
<td></td>
</tr>
<tr>
<td>■ Approval Administrator</td>
<td></td>
</tr>
<tr>
<td>■ Catalog Administrator</td>
<td></td>
</tr>
<tr>
<td>■ Container Administrator</td>
<td></td>
</tr>
<tr>
<td>■ Container Architect</td>
<td></td>
</tr>
<tr>
<td>■ Health Consumer</td>
<td></td>
</tr>
<tr>
<td>■ Infrastructure Architect</td>
<td></td>
</tr>
<tr>
<td>■ Secure Export Consumer</td>
<td></td>
</tr>
<tr>
<td>■ Software Architect</td>
<td></td>
</tr>
<tr>
<td>■ Tenant Administrator</td>
<td></td>
</tr>
<tr>
<td>■ XaaS Architect</td>
<td></td>
</tr>
</tbody>
</table>
Table 1-84. vRealize Automation Appliance Management. This interface is sometimes called the Virtual Appliance Management Interface (VAMI).

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use vRealize Automation Appliance Management for these tasks.</td>
<td>1. Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td></td>
</tr>
<tr>
<td>- View the status of registered services.</td>
<td>2. Click vRealize Automation Appliance Management.</td>
<td>You can also use this URL to open vRealize Automation Appliance Management:</td>
</tr>
<tr>
<td>- View system information and reboot or shutdown the appliance.</td>
<td></td>
<td><a href="https://vra-va-hostname.domain.name:5480">https://vra-va-hostname.domain.name:5480</a>.</td>
</tr>
<tr>
<td>- Manage participation in the Customer Experience Improvement Program.</td>
<td></td>
<td>3. Log in.</td>
</tr>
<tr>
<td>- View network status.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- View update status and install updates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Manage administration settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Manage vRealize Automation host settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Manage SSO settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Manage product licenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configure the vRealize Automation Postgres database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configure vRealize Automation messaging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configure vRealize Automation logging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Install IaaS components.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Migrate from an existing vRealize Automation installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Manage IaaS component certificates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configure Xenon service.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-85. vRealize Orchestrator Client

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Orchestrator Client for these tasks.</td>
<td>1. Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td></td>
</tr>
<tr>
<td>- Develop actions.</td>
<td>2. To download the client.jnlp file to your local computer, click vRealize Orchestrator Client.</td>
<td></td>
</tr>
<tr>
<td>- Develop workflows.</td>
<td>3. Right-click the client.jnlp file and select Launch.</td>
<td>You must be a user with the system administrator role or part of the vcoadmins group configured in the vRealize Orchestrator Control Center Authentication Provider settings.</td>
</tr>
<tr>
<td>- Manage policies.</td>
<td>4. On the Do you want to Continue? dialog box, click Continue.</td>
<td></td>
</tr>
<tr>
<td>- Install packages.</td>
<td>5. Log in.</td>
<td></td>
</tr>
<tr>
<td>- Manage user and user group permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Attach tags to URI objects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- View inventory.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-86. vRealize Orchestrator Control Center

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the vRealize Orchestrator Control Center to edit the configuration of the default vRealize Orchestrator instance that is embedded in vRealize Automation. | 1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name. | User Name  
- Enter root if role-based authentication is not configured.  
- Enter your vRealize Automation user name if it is configured for role-based authentication. |
| | 2 Click vRealize Automation Appliance Management. |  
You can also use this URL to open vRealize Automation Appliance Management: https://vra-va-hostname.domain.name:5480. |
| | 3 Log in. | Password  
- Enter the password you entered when you deployed the vRealize Automation appliance if role-based authentication is not configured.  
- Enter the password for your user name if your user name is configured for role-based authentication. |
| | 4 Click vRA Settings > Orchestrator. |  
5 Select Orchestrator user interface.  
6 Click Start.  
7 Click the Orchestrator user interface URL.  
8 Log in. | |

### Table 1-87. Linux Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the Linux command prompt on a host, such as the vRealize Automation appliance host, for these tasks.  
- Stop or start services  
- Edit configuration files  
- Run commands  
- Retrieve data | 1 On the vRealize Automation appliance host, open a command prompt.  
One way to open the command prompt on your local computer is to start a session on the host using an application such as PuTTY. |  
- User name: root  
- Password: Password you created when you deployed the vRealize Automation appliance. |
| | 2 Log in. | |

### Table 1-88. Windows Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You can use a Windows command prompt on a host, such as the IaaS host, to run scripts. | 1 On the IaaS host, log in to Windows.  
One way to log in from your local computer is to start a remote desktop session. |  
- User name: User with administrative privileges.  
- Password: User’s password. |
| | 2 Open the Windows command prompt.  
One way to open the command prompt is to right-click the Start icon on the host and select Command Prompt or Command Prompt (Admin). | |
Upgrading VMware Products Integrated with vRealize Automation

You must manage any VMware products integrated with your vRealize Automation environment when you upgrade vRealize Automation.

If your vRealize Automation environment is integrated with one or more additional products, you should upgrade vRealize Automation before you update the additional products. If vRealize Business for Cloud is integrated with vRealize Automation, you must unregister vRealize Business for Cloud before you upgrade vRealize Automation.

Follow the suggested workflow for managing integrated products when you upgrade vRealize Automation.

1. Upgrade vRealize Automation.
2. Upgrade VMware vRealize Operations Manager.
3. Upgrade VMware vRealize Log Insight.

This section provides additional guidance for managing vRealize Business for Cloud when it is integrated with your vRealize Automation environment.

Upgrading vRealize Operations Manager Integrated with vRealize Automation

Upgrade vRealize Operations Manager after you upgrade vRealize Automation.

Procedure

1. Upgrade vRealize Automation.
2. Upgrade vRealize Operations Manager. For information, see Updating Your Software in the VMware vRealize Operations Manager Documentation.

Upgrading vRealize Log Insight Integrated with vRealize Automation

Upgrade vRealize Log Insight after you upgrade vRealize Automation.

Procedure

1. Upgrade vRealize Automation.
2. Upgrade vRealize Log Insight. For information, see Upgrading vRealize Log Insight in the VMware vRealize Log Insight Documentation.

Upgrading vRealize Business for Cloud Integrated with vRealize Automation

When you upgrade your vRealize Automation environment, you must unregister and register your connection to vRealize Business for Cloud.

Perform this procedure to ensure continuity of service with vRealize Business for Cloud when you upgrade your vRealize Automation environment.
Procedure


2. Upgrade vRealize Automation.


Preparing to Upgrade vRealize Automation

You must perform various tasks and procedures before you upgrade vRealize Automation from 6.2.5 to 7.4.

Perform the tasks in the order they appear in the upgrade checklist. See Checklist for Upgrading vRealize Automation.

Backup Prerequisites for Upgrading vRealize Automation

Finish the backup prerequisites before you upgrade vRealize Automation 6.2.5 to 7.4.

Prerequisites

- Verify that your source environment is fully installed and configured.
- For each appliance in the source environment, back up all the vRealize Automation appliance configuration files in the following directories.
  - /etc/vcac/
  - /etc/vco/
  - /etc/apache2/
  - /etc/rabbitmq/
- Back up the vRealize Automation external workflow configuration (xmldb) files on your system. Store the backup files in a temporary directory. These files are at \VMware\vCA\Server\ExternalWorkflows\xmldb\. You restore the xmldb files on your new system after migration. See Restore External Workflow Timeout Files.
  
  For a related problem, see Backup Copies of .xml Files Cause the System to Time Out.
Back up the external vRealize Automation PostgreSQL database. To see if your PostgreSQL database is external, complete these steps.


   For a distributed environment, log in to the primary vRealize Automation appliance management console.

b. Select vRA Settings > Database.

c. If the vRealize Automation PostgreSQL database node host is different from the vRealize Automation appliance host, back up the database. If the database node host is the same as the appliance host, you do not need to back up the database.

   For information about the PostgreSQL database backup, see https://www.postgresql.org/.

- Create a snapshot of your tenant configuration and the users assigned.
- Back up any files you have customized, such as DataCenterLocations.xml.
- Create a snapshot of each virtual appliance and IaaS server. Adhere to regular guidelines for backing up the entire system in case the vRealize Automation upgrade is unsuccessful. See Backup and Recovery for vRealize Automation Installations.

**Back Up Your Existing vRealize Automation 6.2.5 Environment**

Before you upgrade, shut down and take a snapshot of your vRealize Automation 6.2.5 environment components.

Before you upgrade, take a snapshot of these components while your system is shut down.

- vRealize Automation IaaS servers (Windows nodes)
- vRealize Automation appliances (Linux nodes)
- vRealize Automation (SSO) Identity node

If the upgrade fails, use the snapshot to return to the last known good configuration and attempt another upgrade.

**Prerequisites**

- Verify that the embedded PostgreSQL database is in high-availability mode. If it is, locate the current Master node. See the knowledge base article http://kb.vmware.com/kb/2105809.
- If your environment has an external PostgreSQL database, create a database backup file.
- If the vRealize Automation Microsoft SQL database is not hosted on the IaaS server, create a database backup file. For information, find article on the Microsoft Developer Network about creating a full SQL Server database backup.
- Verify that you have completed the backup prerequisites for upgrading.
- Verify that you have taken a snapshot of your system while it is shut down. This is the preferred method of taking a snapshot. See your vSphere 6.0 Documentation.

  **Note**  When you back up the vRealize Automation appliance and the IaaS components, disable in-memory snapshots and quiesced snapshots.

- If you modified the `app.config` file, make a backup of that file. See Restore Changes to Logging in the `app.config` File.

- Make a backup of the external workflow configuration (xml$db) files. See Restore External Workflow Timeout Files.

- Verify that you have a location outside your current folder where you can store your backup file. See Backup Copies of .xml Files Cause the System to Time Out.

**Procedure**

1. Log in to your vCenter Server.

2. Locate these vRealize Automation 6.2.5 components.
   - vRealize Automation IaaS servers (Windows nodes)
   - vRealize Automation appliances (Linux nodes)
   - vRealize Automation (SSO) Identity node

3. For each of the following virtual machines, select the virtual machine, click **Shutdown guest**, and wait for the virtual machine to stop. Shut down these virtual machines in the following order.
   a. IaaS proxy agent virtual machines
   b. DEM Worker virtual machines
   c. DEM Orchestrator virtual machine
   d. Manager Service virtual machine
   e. Web Service virtual machines
   f. Secondary vRealize Automation virtual appliances
   g. Primary vRealize Automation virtual appliance
   h. Manager virtual machines (if any)
   i. Identity Appliance

4. Take a snapshot of each vRealize Automation 6.2.5 virtual machine.

5. Clone each vRealize Automation appliance node.
   You perform the upgrade on the cloned virtual machines.

6. Power off each original vRealize Automation appliance virtual machine before you upgrade the cloned virtual machines.
   Keep the original virtual machines powered off and use them only if you must restore the system.
What to do next

Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5.

Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5

Before you upgrade from vRealize Automation 6.2.5, you must increase hardware resources for each vRealize Automation appliance.

This procedure assumes that you use the Windows vCenter Server client.

Prerequisites

- Verify that you have a clone of each vRealize Automation appliance.
- Verify that you have at least 140 GB of free space in your vCenter Server for each appliance clone.
- Verify that the original appliances are powered off.

Procedure

1. Log in to vCenter Server.
2. Right-click a cloned vRealize Automation appliance icon and select **Edit Settings**.
3. Select **Memory** and set the value to 18 GB.
4. Select **CPU** and set the **Number of virtual sockets** value to 4.
5. Extend the size of virtual Disk 1 to 50 GB.
   a. Select Disk 1.
   b. Change the size to 50 GB.
   c. Click **OK**.
6. If you do not have Disk 3, complete these steps to add a Disk 3 with a disk size of 25 GB.
   a. Click **Add** above the Resources table to add a virtual disk.
   b. Select **Hard Disk** for the **Device Type**, and click **Next**.
   c. Select **Create a new virtual disk**, and click **Next**.
   d. Set **disk size** value to 25 GB.
   e. Select **Store with the virtual machine** and click **Next**.
   f. Verify that the **Independent** option is deselected for **Mode** and **SCSI (0:2)** is selected for **Virtual Device Mode**, and click **Next**.
      If prompted to accept recommended settings, accept the recommended settings.
   g. Click **Finish**.
   h. Click **OK**.
7 If there is an existing virtual Disk 4 from a previous vRealize Automation release, complete these steps.
   
a Power on the primary virtual appliance clone and wait 1 minute.
   
b Power on the secondary virtual appliance clone.
   
c On the primary virtual appliance clone, open a new command prompt and navigate to `/etc/fstab`.
   
d On the primary virtual appliance clone, open the `fstab` file, and remove lines starting with `/dev/sdd` that contain the Wal_Archive write ahead logs.
   
e On the primary virtual appliance clone, save the file.
   
f On the secondary virtual appliance clone, open a new command prompt and navigate to `/etc/fstab`.
   
g On the secondary virtual appliance clone, open the `fstab` file, and remove lines starting with `/dev/sdd` that contain the Wal_Archive write ahead logs.
   
h On the secondary virtual appliance clone, save the file.
   
i Power off the secondary virtual appliance clone and wait 1 minute.
   
j Power off the primary virtual appliance clone.
   
k Right-click the cloned vRealize Automation primary appliance icon and select Edit Settings.
   
l Delete Disk 4 on the cloned primary virtual appliance machine.
   
m Right-click the cloned vRealize Automation secondary appliance icon and select Edit Settings.
   
n Delete Disk 4 on the cloned secondary virtual appliance machine.

8 Complete these steps to add a Disk 4 with a disk size of 50 GB to the cloned primary and secondary virtual appliance machines.
   
a Click Add above the Resources table to add a virtual disk.
   
b Select Hard Disk for the Device Type, and click Next.
   
c Select Create a new virtual disk, and click Next.
   
d Set disk size value to 50 GB.
   
e Select Store with the virtual machine and click Next.
   
f Verify that the Independent option is deselected for Mode and SCSI (0:3) is selected for Virtual Device Mode, and click Next.
      If prompted to accept recommended settings, accept the recommended settings.
   
g Click Finish.
   
h Click OK.

9 Create a snapshot of the cloned primary virtual appliance machine and the cloned secondary virtual appliance machine.
What to do next

Power On the Entire System.

Power On the Entire System
After you increase the vCenter hardware resources for upgrade, you power on the system before you perform the upgrade.

Prerequisites
- Back Up Your Existing vRealize Automation 6.2.5 Environment.
- Increase vCenter Server Hardware Resources for vRealize Automation 6.2.5.

Procedure
1. Power on the entire system.
   
   For instructions, see the vRealize Automation 6.2 version of the Start Up vRealize Automation topic.

   **Note** If you have a high-availability environment, use this procedure to power on your virtual appliances.
   
   a. Power on the virtual appliance that you powered off last.
   b. Wait one minute.
   c. Power on the remaining virtual appliances.

2. Verify that the system is fully functional.

What to do next

Stop vRealize Automation Services on the IaaS Windows Server.

Stop vRealize Automation Services on the IaaS Windows Server
When necessary, you can use the following procedure to stop vRealize Automation services on each server that is running IaaS services.

Before you begin the upgrade, stop vRealize Automation services on each IaaS Windows server.

**Note** Except for a passive backup instance of the Manager Service, the startup type for all services must be set to Automatic during the upgrade process. If you set services to Manual, the upgrade process fails.

Procedure
1. Log in to your IaaS Windows server.
2. Select **Start > Administrative Tools > Services**.
3. Stop services in the following order. Be careful not to shut down the virtual machine.
   
   Each virtual machine has a Management agent, which must be stopped with each set of services.
   
   a. Each VMware vCloud Automation Center Agent
b Each VMware DEM-Worker

c The VMware DEM-Orchestrator

d The VMware vCloud Automation Center Service

4 For distributed deployments with load balancers, disable each secondary node and remove the vRealize Automation health monitors for the following items.

a vRealize Automation appliance

b IaaS Website

c IaaS Manager Service

Verify that load balancer traffic is directed only to the primary nodes and that the vRealize Automation health monitors are removed for the appliance, Website, and Manager Service, otherwise the upgrade fails.

5 Verify that the IaaS service hosted in Microsoft Internet Information Services (IIS) is running by performing the following steps.

a In your browser, go to the URL https://webhostname/Repository/Data/MetaModel.svc to verify that the Web Repository is running. If successful, no errors are returned and you see a list of models in XML format.

b Check the status recorded in the Repository.log file on the Web node of the IaaS virtual machine to see that status reports OK. The file is located in the VCAC home folder at /Server/Model Manager Web/Logs/Repository.log.

For a distributed IaaS Website, log in to the secondary Website, without MMD, and stop the Microsoft IIS server temporarily. Check the MetaModel.svc connectivity. To verify that the load balancer traffic is going through only the primary Web node, start the Microsoft IIS server.

What to do next

Downloading vRealize Automation Appliance Updates.

Downloading vRealize Automation Appliance Updates

You can check for updates on your appliance management console, and download the updates using one of the following methods.

For best upgrade performance, use the ISO file method.

To avoid potential problems when upgrading your appliance, or if issues arise during appliance upgrade, see VMware Knowledge Base article vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database (54987).

- Download vRealize Automation Appliance Updates from a VMware Repository

  You can download the update for your vRealize Automation appliance from a public repository on the vmware.com website.
Download Virtual Appliance Updates for Use with a CD-ROM Drive

You can update your virtual appliance from an ISO file that the appliance reads from the virtual CD-ROM drive. This is the preferred method.

Download vRealize Automation Appliance Updates from a VMware Repository

You can download the update for your vRealize Automation appliance from a public repository on the vmware.com website.

Prerequisites

- Back up your existing vRealize Automation environment.
- Verify that your vRealize Automation appliance is powered on.

Procedure

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
2. Click the Update tab.
3. Click Settings.
4. (Optional) Set how often to check for updates in the Automatic Updates panel.
5. Select Use Default Repository in the Update Repository panel.
   - The default repository is set to the correct VMware.com URL.
6. Click Save Settings.

Download Virtual Appliance Updates for Use with a CD-ROM Drive

You can update your virtual appliance from an ISO file that the appliance reads from the virtual CD-ROM drive. This is the preferred method.

You download the ISO file and set up the primary appliance to use this file to upgrade your appliance.

Prerequisites

- Back up your existing vRealize Automation environment.
- Verify that all CD-ROM drives you use in your upgrade are enabled before you update a vRealize Automation appliance. See the vSphere documentation for information about adding a CD-ROM drive to a virtual machine in the vSphere client.

Procedure

1. Download the update repository ISO file.
   b. Click vRealize Automation Download Resources to go to the VMware download page.
   c. Download the appropriate file.
2 Locate the downloaded file on your system to verify that the file size is the same as the file on the VMware download page. Use the checksums provided on the download page to validate the integrity of your downloaded file. For information, see the links at the bottom of the VMware download page.

3 Verify that your primary virtual appliance is powered on.

4 Connect the CD-ROM drive for the primary virtual appliance to the ISO file you downloaded.

5 On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.

6 Click the Update tab.

7 Click Settings.

8 Under Update Repository, select Use CDROM Updates.

9 Click Save Settings.

**Updating the vRealize Automation Appliance**

After you complete the upgrade prerequisites and download the virtual appliance update, you update the vRealize Automation 6.2.5 Appliance to 7.4. You also reconfigure some settings for the primary vRealize Automation appliance.

After you upgrade the primary vRealize Automation appliance, you upgrade the other nodes in your environment in the following order:

1. Each secondary vRealize Automation appliance
2. IaaS Web site
3. IaaS Manager Service
4. IaaS DEM
5. IaaS Agent
6. Upgrade or migrate each external vRealize Orchestrator instance

**Install the Update on the vRealize Automation Appliance**

You install the vRealize Automation update on the vRealize Automation 6.2.5 appliance and configure the appliance settings.

Support for an external PostgreSQL database is discontinued beginning with vRealize Automation 7.1. The upgrade process merges the data from an existing PostgreSQL external database with the PostgreSQL internal database that is part of the vRealize Automation appliance.

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

Do not close the management console while you install the update.

If you encounter any problems during the upgrade process, see Troubleshooting the vRealize Automation Upgrade.
Prerequisites

- Verify that you selected a download method and downloaded the update. See Downloading vRealize Automation Appliance Updates.
- For high-availability distributed deployments, see Back Up Your Existing vRealize Automation 6.2.5 Environment.
- For deployments with load balancers, verify that the traffic is directed only to the primary node and that the health monitors are disabled.
- If you have a Common Components Catalog component installed in your environment, uninstall the component before you upgrade. For information, see the Common Components Catalog Installation Guide. If this guide is unavailable, use the alternative procedure in the Checklist for Upgrading vRealize Automation.
- Verify that the jdbc:postgresql database connection points to the external IP address of the master PostgreSQL node.
  a  On each vRealize Automation appliance, open a new command prompt.
  b  Navigate to /etc/vcac/server.xml, and back up server.xml.
  c  Open server.xml.
  d  If necessary, edit the server.xml file entry jdbc:postgresql that points to the Postgres database and point it to the external IP address of the master PostgreSQL node for external PostgreSQL or primary virtual appliance for embedded PostgreSQL.
    For example, jdbc:postgresql://198.15.100.60:5432/vcac
- Verify that all saved and in-progress requests have finished successfully before you upgrade.

Procedure

1  Open the vRealize Automation appliance management console.
   a  On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
   b  Log in with the user name root and the password you entered when you deployed the appliance.
2  Click Services and verify that each service, except iaas-service, is listed as REGISTERED.
3  Select Update > Settings.
4  Select one of the following:
   - Use Default Repository.
   - Use CDROM Updates.
5  Click Save Settings.
6  Select Status.
7 Click **Check Updates** to verify that an update is accessible.

8 (Optional) For instances of vRealize Automation appliance, click **Details** in the Appliance Version area to see information about the location of release notes.

9 Click **Install Updates**.

10 Click **OK**.

A message stating that the update is in progress appears.

11 (Optional) If you have not resized Disk 1 to 50 GB manually, perform the following steps.

   a When the system prompts you to reboot the virtual appliance, click **System** and click **Reboot**. During the reboot, the system adjusts the space required for the update.

   b After the system reboots, log in again to the vRealize Automation appliance management console, verify that each service, except iaas-service, is listed as REGISTERED, and select **Update > Status**.

   c Click **Check Updates** and **Install Updates**.

12 To view the upgrade progress, open the following log files.

   - /opt/vmware/var/log/vami/updatecli.log
   - /opt/vmware/var/log/vami/vami.log
   - /var/log/vmware/horizon/horizon.log
   - /var/log/bootstrap/*.log

   If you log out during the upgrade process and log in again before the upgrade is finished, you can continue to follow the progress of the update in the log file. The updatecli.log file might display information about the version of vRealize Automation that you are upgrading from. This displayed version changes to the proper version later in the upgrade process.

   The time required for the update to finish varies according to your environment.

13 Click **Telemetry** in the appliance management console. Read the note about participation in the Customer Experience Improvement Program (CEIP) and select to join or not join the program.

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

For more information about the Customer Experience Improvement Program, see Join or Leave the Customer Experience Improvement Program for vRealize Automation.

**What to do next**

*Update Your Single Sign-On Password for VMware Identity Manager.*

**Update Your Single Sign-On Password for VMware Identity Manager**

After you install the updates, you must update the Single Sign-On password for VMware Identity Manager.
VMware Identity Manager replaces the Identity Appliance and vSphere SSO components.

**Procedure**

1. Log out of the vRealize Automation appliance management console, close the browser, open the browser again, and log back in.

2. Select **vRA Settings > SSO**.

3. Enter a new VMware Identity Manager password and click **Save Settings**.
   
   Do not use simple passwords. You can safely ignore the error message *SSO server is not connected. It can require several minutes to restart the services.*
   
   The password is accepted.
   
   For a high-availability deployment, the password is applied to the first vRealize Automation appliance node and propagated to all secondary vRealize Automation appliance nodes.

4. Reboot the virtual appliance.
   
   a. Click the **System** tab.
   
   b. Click **Reboot** and confirm your selection.

5. Verify that all services are running.
   
   a. Log in to the vRealize Automation appliance management console.
   
   b. Click the **Services** tab on the console.
   
   c. Click the **Refresh** tab to monitor the progress of service startup.
   
   You should see a minimum of 35 services.

6. Verify that all services are registered except iaas-service.
   
   The release-management service does not start without a vRealize Code Stream license key.

**What to do next**

**Update the License Key.**

**Update the License Key**

You must upgrade your license key to use the latest version of the vRealize Automation appliance.

**Procedure**


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

3. Select **vRA Settings > Licensing**.
   
   If the **Licensing** tab is not available, perform the following steps and repeat the procedure.
   
   a. Log out of the management console.
b Clear your browser cache.

4 Enter your new license key in the New License Key text box.

Endpoints and quotas are flagged according to your end-user license agreement (EULA).

5 Click Submit Key.

What to do next

Migrate Identity Stores to VMware Identity Manager.

Migrate Identity Stores to VMware Identity Manager

When you upgrade from vRealize Automation 6.2.5 to the current version, you must migrate the identity stores.

As required in the following procedures, refer to the snapshot of your 6.2.5 tenant configuration information.

Note After you migrate the identity stores, users of vRealize Code Stream must manually reassign vRealize Code Stream roles.

Procedure

1 Create a Local User Account for Your Tenants

You must set up a tenant with a local user account and assign tenant administrator privileges to the local user account.

2 Synchronize Users and Groups for an Active Directory Link

To import your users and groups into vRealize Automation using the Directories Management capability, you must connect to your Active Directory link.

3 Migrate Custom Groups to the Target VMware Identity Manager

You must migrate all custom groups from the source environment to the VMware Identity Manager (vIDM) in the target deployment.

4 Migrate Multiple Tenant and IaaS Administrators

For each vRealize Automation tenant with Tenant or IaaS administrators, you must delete and restore each administrator manually.

Create a Local User Account for Your Tenants

You must set up a tenant with a local user account and assign tenant administrator privileges to the local user account.

Repeat this procedure for each of your tenants.

Prerequisites

Verify that you have set a new VMware Identity Manager password. See Update Your Single Sign-On Password for VMware Identity Manager.
Procedure

1. Log in to the vRealize Automation console with the default system administrator user name `administrator` and password.

   The console location is `https://vra-appliance/vcac/`.

2. Click your tenant.

   For example, for the default tenant, click `vsphere.local`.

3. Select the Local Users tab.

4. Click New.

5. Create a local user account.

   You assign the tenant administrator role to this user. Verify that the local user name is unique to the vsphere.local active directory.

6. Click OK.

7. Click Administrators.

8. Enter the local user name in the Tenant administrators search box and press Enter.

9. Click Finish.

10. Log out of the console.

What to do next

   Synchronize Users and Groups for an Active Directory Link.

Synchronize Users and Groups for an Active Directory Link

To import your users and groups into vRealize Automation using the Directories Management capability, you must connect to your Active Directory link.

Perform this procedure for each of your tenants.

Prerequisites

Verify that you have access privileges to the Active Directory.

Procedure

1. Log in to the vRealize Automation console at: `https://vra-appliance/vcac/org/tenant_name`.

2. Select Administration > Directories Management > Directories.

3. Click Add Directory and select Add Active Directory over LDAP/IWA.
4 Enter your Active Directory account settings.

- **Non-Native Active Directories**

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name. Select Active Directory over LDAP when using non-Native Active Directory.</td>
</tr>
<tr>
<td>This Directory Supports DNS Services</td>
<td>Deselect this option.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the Distinguished Name (DN) of the starting point for directory server searches. For example, <code>cn=users,dc=rainpole,dc=local</code>.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>Enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users. For example, <code>cn=config_admin_infra,cn=users,dc=rainpole,dc=local</code>.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory password for the account that can search for users.</td>
</tr>
</tbody>
</table>

- **Native Active Directories**

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name. Select Active Directory (Integrated Windows Authentication) when using Native Active Directory.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the name of the domain to join.</td>
</tr>
<tr>
<td>Domain Admin Username</td>
<td>Enter the user name for the domain admin.</td>
</tr>
<tr>
<td>Domain Admin Password</td>
<td>Enter the password for the domain admin account.</td>
</tr>
<tr>
<td>Bind User UPN</td>
<td>Use the email address format to enter the name of the user who can authenticate the domain.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory bind account password for the account that can search for users.</td>
</tr>
</tbody>
</table>

5 Click **Test Connection** to test the connection to the configured directory.

6 Click **Save & Next**.

The **Select the Domains** page appears, and displays the list of domains.

7 Accept the default domain setting and click **Next**.

8 Verify that the attribute names are mapped to the correct Active Directory attributes, and click **Next**.

9 Select the groups and users to synchronize.
   
   a Click the **New** icon.
   
   b Enter the user domain and click **Find Groups**.
      
      For example, enter `dc=vcac, dc=local`.
   
   c To select the groups to synchronize, click **Select** and click **Next**.
   
   d On the **Select Users** page, select the users to synchronize and click **Next**.
10 Review the users and groups are syncing to the directory, and click **Sync Directory**.

   The directory synchronization takes some time and runs in the background.

11 Select **Administration > Directories Management > Identity Providers**, and click your new identity provider.

   For example, **WorkspaceIDP__1**.

12 Scroll to the bottom of the page, and update the value for the IdP Hostname property to point to the FQDN for the vRealize Automation load balancer.

13 Click **Save**.

14 Repeat steps 11–13 for each tenant and identity provider.

15 After you upgrade all vRealize Automation nodes, log in to each tenant and select **Administration > Directories Management > Identity Providers**.

   Each identity provider has all vRealize Automation connectors added to it.

   For example, if your deployment has two vRealize Automation appliances, the identity provider has two associated connectors.

**Migrate Custom Groups to the Target VMware Identity Manager**

You must migrate all custom groups from the source environment to the VMware Identity Manager (vIDM) in the target deployment.

Complete this procedure to migrate custom groups.

**Prerequisites**

- Create a Local User Account for Your Tenants.
- Ensure that the horizon-workspace service is running on the vRealize Automation virtual appliance.

**Procedure**

1 Start an SSH session on the vRealize Automation virtual appliance.

2 At the command prompt, log in as **root** with the password you created when you installed the vRealize Automation virtual appliance.

3 Run this command.

   `vcac-config migrate-custom-groups`

   - This message appears when migration completes: The migration of Custom Groups completed successfully!
   - This message appears if no custom groups are in your source environment: No Custom Groups were found in vRA database. Migration process will be skipped.

**Note**  If custom group migration fails, view the log file at `/var/log/vmware/vcac/vcac-config.log` for details.
**Migrate Multiple Tenant and IaaS Administrators**

For each vRealize Automation tenant with Tenant or IaaS administrators, you must delete and restore each administrator manually.

Perform the following procedure for each tenant in the vRealize Automation console.

**Prerequisites**

Log in to the vRealize Automation console on the upgraded virtual appliance.

   
   For a distributed environment, open the console on the master virtual appliance.
2. Select the vsphere.local domain.
3. Log in with the user name administrator and the password that you entered when you deployed the virtual appliance.

**Procedure**

1. Select Administration > Tenants.
2. Click a tenant name.
3. Click Administrators.
4. Make a list of each tenant and IaaS administrator name and user name.
5. Point to each administrator and click the delete icon (X) until you delete all administrators.
6. Click Finish.
7. On the Tenants page, click the tenant name again.
8. Click Administrators.
9. Enter the name of each user that you deleted in the appropriate search box and press Enter.
10. Click the name of the appropriate user from the search returns to add the user back as an administrator.

   When you finish, the list of tenant administrators and IaaS administrators looks the same as the list of administrators you deleted.
11. Click Finish.

**What to do next**

Upgrade the secondary appliances. See Install the Update on Additional vRealize Automation Appliances.
Install the Update on Additional vRealize Automation Appliances

In a high-availability environment, the master virtual appliance is the node that runs the embedded PostgreSQL database in the Master mode. The other nodes in the environment run the embedded PostgreSQL database in Replica mode. During upgrade, the replica virtual 6.2.5 appliance does not require database changes.

Do not close the management console while you install the update.

Prerequisites

- Verify that you have downloaded the virtual appliance updates. See Downloading vRealize Automation Appliance Updates.
- Verify that the jdbc:postgresql database connection points to the external IP address of the master PostgreSQL node.
  a. On the vRealize Automation appliance, open a new command prompt.
  b. Navigate to /etc/vcac/server.xml, and back up the server.xml file.
  c. Open the server.xml file.
  d. If necessary, edit the server.xml file entry jdbc:postgresql to indicate the PostgreSQL database that you want to use.
    - For an external PostgreSQL database, enter the external IP address of the master PostgreSQL node.
    - For the embedded PostgreSQL database, enter the IP address of the master virtual appliance.
      For example, jdbc:postgresql://198.15.100.60:5432/vcac

Procedure

1. Open the vRealize Automation appliance management console for the upgrade.
   a. On each secondary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
   b. Log in with the user name root and the password you entered when you deployed the appliance.
   c. Click Update.
2. Click Settings.
3. Select to download the updates from a VMware repository or CDROM in the Update Repository section.
4. Click Status.
5. Click Check Updates to verify that an update is accessible.
6. Click Install Updates.
7 Click OK.

A message stating that the update is in progress appears.

8 (Optional) If you have not manually resized Disk 1 GB to 50 GB, perform the following steps.
   a When the system prompts you to reboot the virtual appliance, click System and click Reboot.
   During the reboot, the system adjusts the space on Disk 1 required for the update.
   b After the system reboots, log out and log in again to the vRealize Automation appliance management console and select Update > Status.
   c Click Check Updates and Install Updates.

9 To verify that upgrade is progressing successfully, open the log files.
   - /opt/vmware/var/log/vami/vami.log
   - /opt/vmware/var/log/vami/updatecli.log
   - /var/log/vmware/horizon/horizon.log
   - /var/log/bootstrap/*.log

   If you log out during the upgrade process and log in, you can continue to follow the progress of the update in the log file /opt/vmware/var/log/vami/updatecli.log.

   The time it takes for the update to finish depends on your environment.

10 When the update is finished, log out the vRealize Automation appliance management console, clear your Web browser cache, and log in to the vRealize Automation appliance management console.

11 Reboot the virtual appliance.
   a Click System.
   b Click Reboot and confirm your selection.

12 After the virtual appliance has rebooted, log in to the replica vRealize Automation appliance management console.

13 Select vRA Settings > Cluster.

14 Enter the master vRealize Automation appliance user name and password.

15 Click Join Cluster.

16 Click Services and verify that each service, except iaas-service, is listed as REGISTERED.

What to do next

Upgrading the IaaS Server Components After Upgrading vRealize Automation.

Upgrading the IaaS Server Components After Upgrading vRealize Automation

After you upgrade vRealize Automation from 6.2.5 to 7.4, a system administrator upgrades the IaaS server components, including the Microsoft SQL Server database.
You have two options for upgrading the IaaS server components.

- Use the automated IaaS upgrade shell script.
- Use the vRealize Automation 7.4 IaaS installer executable file.

If you have a Common Components Catalog component installed, you must uninstall the component before you upgrade. After you finish the upgrade, you can reinstall the component with the appropriate version. For more information, see the Common Components Catalog Installation Guide. If this guide is unavailable, use the alternative procedure in Checklist for Upgrading vRealize Automation.

**Upgrade IaaS Components Using the Upgrade Shell Script**

Use the upgrade shell script to upgrade the IaaS Components after you update each vRealize Automation 6.2.5 appliance to 7.4.

The updated primary or master vRealize Automation appliance contains a shell script that you use to upgrade each IaaS node and component.

You can run the upgrade script by using the vSphere console for the virtual machine or by using an SSH console session. If you use the vSphere console, you avoid intermittent network connectivity problems that can break the execution of the script.

If you stop the script while the script is upgrading a component, the script runs until the upgrade is finished on the component. If any components on the node are not upgraded, you must run the script again.

When the upgrade finishes, you can review the upgrade result by opening the upgrade log file at `/usr/lib/vcac/tools/upgrade/upgrade.log`.

**Prerequisites**

- Verify the successful update of all vRealize Automation appliances.
- If you reboot an IaaS server after you update all the vRealize Automation appliances, you must stop the IaaS Windows services. Before you upgrade the IaaS components, stop all the IaaS Windows services, except for the Management Agent service, on the server.
- Before you run the upgrade shell script on the master or primary vRealize Automation appliance node, verify that each service is REGISTERED.
  a. Go to the appliance management console for your virtual appliance by using its fully qualified domain name: `https://va-hostname.domain.name:5480`.
  b. Log in with the user name `root` and the password you entered when the appliance was deployed.
  c. Click **Services**.
  d. Verify that each service, except the iaas-service, is REGISTERED.
- Upgrade the Management Agent on each vRealize Automation IaaS virtual machine.
  a. Open a browser and navigate to the VMware vRealize Automation IaaS Installation page on the vRealize Automation appliance using the fully qualified domain name: `https://virtual_appliance_host:5480/installer`.
b Click **Management Agent Installer**.

By default, the installer is downloaded to the Downloads folder.

c Log in to each vRealize Automation IaaS virtual machine, upgrade the Management Agent with the **Management Agent Installer** file.

- Verify that your primary IaaS Website node where the Model Manager data is installed has JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, you must set the environment variable, JAVA_HOME, to the new version.

- Log in to each IaaS Website node and verify that the creation date is earlier than the modified date in the `web.config` file. If the creation date for the `web.config` file is the same as or later than the modified date, perform the procedure in **Upgrade Fails for IaaS Website Component**.

- To verify that each IaaS node has an upgraded IaaS Management Agent, perform these steps on each IaaS node.

  a Log in to the vRealize Automation appliance management console.

  b Select **vRA Settings > Cluster**.

  c Expand the list of all installed components on each IaaS node, and locate the IaaS Management Agent.

  d Verify that the Management Agent version is current.

- Verify that the IaaS Microsoft SQL Server database backup is accessible in case you must roll back.

- Delete all orphaned IaaS nodes. See **Delete Orphaned Nodes on vRealize Automation**.

- Verify that snapshots of the IaaS servers in your deployment are available.

  If the upgrade is unsuccessful, return to the snapshot and database backup and attempt another upgrade.

**Procedure**

1 Open a new console session on the primary or master vRealize Automation appliance node and log in with the root account.

   If you plan to run the upgrade script with SSH, open an SSH console session.

2 Change directories to `/usr/lib/vcac/tools/upgrade/`.

3 At the prompt, run this command to create the `upgrade.properties` file.

   ```
   ./generate_properties
   ```

4 Open the `upgrade.properties` file and enter all the required values.

   This table shows the required values, which vary depending on the environment. For example, on a node that contains a DEM worker or orchestrator, DEM credentials are required.
### Required Value

<table>
<thead>
<tr>
<th>Description</th>
<th>Credential Format</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name for the primary Web node. Required only once.</td>
<td>DomainUser</td>
<td>iaasDomain\webuser</td>
</tr>
<tr>
<td>Password for the primary Web node. Required only once.</td>
<td>Password</td>
<td>pa$$w0rd!</td>
</tr>
<tr>
<td>User name for the DEM worker or DEM orchestrator. Required for each node where a DEM component is installed.</td>
<td>DomainUser</td>
<td>iaasDomain\demuser</td>
</tr>
<tr>
<td>Password for the DEM worker or DEM orchestrator. Required for each node where a DEM component is installed.</td>
<td>Password</td>
<td>pa$$w0rd!</td>
</tr>
<tr>
<td>User name for an agent such as a vSphere agent. Required for each node where an agent component is installed.</td>
<td>DomainUser</td>
<td>iaasDomain\agent_user</td>
</tr>
<tr>
<td>Password for an agent such as a vSphere agent. Required for each node where an agent component is installed.</td>
<td>Password</td>
<td>pa$$w0rd!</td>
</tr>
<tr>
<td>The VIDM administrator password. Required only when you upgrade from vRealize Automation 6.2.5.</td>
<td>vIDM_password</td>
<td>pa$$w0rd!</td>
</tr>
</tbody>
</table>

For security reasons, the upgrade.properties file is removed when you run the upgrade shell script. The properties in the file are defined using the information for each IaaS component that comes through the IaaS Management Agents. It is important that all IaaS Management Agents are upgraded and healthy before running the ./generate.properties or ./upgrade_from_62x shell scripts. If any IaaS Management Agent has a problem when you run the upgrade shell script, see Update Fails to Upgrade the Management Agent. To recreate the upgrade.properties file, repeat steps 2 and 3.

5. Run the upgrade script.

   a. At the command prompt, enter ./upgrade_from_62x.

   b. Press Enter.

The script displays each IaaS node and all the components installed on it. The script validates each component before installing the upgrade. If there are incorrect values in the upgrade.properties file, the script fails.

The first IaaS server component can take 30 minutes or longer to finish. During the upgrade, you see a message similar to Upgrading server components for node web1-vra.mycompany.com.

If the upgrade shell script is unsuccessful, review the upgrade.log file.

You can run the upgrade script again after you fix a problem. Before you run the upgrade script again, recreate the upgrade.properties file, open it, and enter all the required values.
6 (Optional) Enable automatic Manager Service failover. See Enable Automatic Manager Service Failover After Upgrade.

What to do next

Restore Access to Built-In vRealize Orchestrator Control Center.

Upgrading IaaS Components Using the IaaS Installer

You can use this alternative method to upgrade IaaS components after upgrading vRealize Automation from 6.2.5 to 7.4.

Download the IaaS Installer to Upgrade IaaS Components

After upgrading from vRealize Automation 6.2.5 to 7.4, download the IaaS installer to the virtual machine where the IaaS components to be upgraded are installed.

If you see certificate warnings during this procedure, you can ignore them.

Note Except for a passive backup instance of the Manager Service, the startup type for all services must be set to Automatic during the upgrade process. If you set services to Manual, the upgrade process fails.

Prerequisites

- Verify that Microsoft .NET Framework 4.5.2 or later is installed on the IaaS installation virtual machine. You can download the .NET installer from the VMware vRealize Automation IaaS Installation page. If you update .NET to 4.5.2 after you shut down the services, the virtual machine might restart as part of the installation. When this happens, you must manually stop all IaaS services on the virtual machine except for the Management Agent.

- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. Enter res://iesetup.dll/SoftAdmin.htm in the search bar and press Enter.

- Log in as a local administrator to the Windows server where one or more of the IaaS components you want to upgrade are installed.

Procedure

1 Open a Web browser.

2 Enter the URL for the VMware vRealize Automation IaaS Installation page.

   For example, https://vcac-va-hostname.domain.name:5480/installer, where vcac-va-hostname.domain.name is the name of the primary or master vRealize Automation appliance node.

3 Click IaaS installer.

4 The installer file, setup__vcac-va-hostname.domain.name@5480.exe, is sent to the Downloads folder by default.

   Do not change the filename. It is used to connect the installation to the vRealize Automation appliance.
What to do next

- If you have a standalone vRealize Orchestrator, see Upgrading Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation.
- If you have an external vRealize Orchestrator appliance cluster, see Upgrading External vRealize Orchestrator Appliance Cluster for Use with vRealize Automation.
- See Upgrade the IaaS Components After Upgrading vRealize Automation.

Upgrade the IaaS Components After Upgrading vRealize Automation

After upgrading vRealize Automation 6.2.5 to 7.4, you must upgrade the SQL database and configure all systems that have IaaS components installed. You can use these steps for minimal and distributed installations.

**Note** The IaaS installer must be on the virtual machine that contains the IaaS components you want to upgrade. You cannot run the installer from an external location, except for the Microsoft SQL database, which also can be upgraded remotely from the Web node.

Verify that snapshots of the IaaS servers in your deployment are available. If the upgrade fails, you can return to the snapshot and attempt another upgrade.

Perform the upgrade so that services are upgraded in the following order:

1. **IaaS Websites**
   - If you are using a load balancer, disable traffic to all non-primary nodes.
   - Finish the upgrade on one server before upgrading the next server that is running a Website service. Begin with the one that has the Model Manager Data component installed.
   - If you are performing a manual external Microsoft SQL database upgrade, you must upgrade the external SQL before you upgrade the Web node. You can upgrade the external SQL remotely from the Web node.

2. **Manager Services**
   - Upgrade the active Manager Service before you upgrade the passive Manager Service.
   - If you do not have SSL encryption enabled in your SQL instance, deselect **SSL encryption** in the IaaS Upgrade configuration dialog box.

3. **DEM orchestrator and workers**
   - Upgrade all DEM orchestrators and workers. Finish the upgrade on one server before you upgrade the next server.

4. **Agents**
   - Finish the upgrade on one server before you upgrade the next server that is running an agent.

5. **Management Agent**
   - Is updated as part of the upgrade process.
If you are using different services on one server, the upgrade updates the services in the proper order. For example, if your site has website and manager services on the same server, select both for update. The upgrade installer applies the updates in the proper order. You must complete the upgrade on one server before you begin an upgrade on another.

**Note** If your deployment uses a load balancer, the first appliance you plan to upgrade must be connected to the load balancer. All other instances of vRealize Automation appliance must be disabled for load balancer traffic before you apply the upgrade to avoid caching errors.

**Prerequisites**

- Back up your existing vRealize Automation 6.2.5 environment.
- If you reboot an IaaS server after you update all the vRealize Automation appliances, you must stop the IaaS Windows services. Before you upgrade the IaaS components, stop all the IaaS Windows services, except for the Management Agent service, on the server.
- **Download the IaaS Installer to Upgrade IaaS Components.**
- Verify that your primary IaaS Website node where the Model Manager data is installed has the proper Java version. You must have JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, set the environment variable, JAVA_HOME, to the new version.
- Verify that the creation date is earlier than the modified date in the *web.config* file. If the creation date for the *web.config* file is the same as or later than the modified date, perform the procedure in Upgrade Fails for IaaS Website Component.
- If you are upgrading from vRealize Automation 6.2.5 and have an external Microsoft SQL database, you must have the proper Management Agent version. The Management Agent on the external database must be version 7.0 or later before you run the IaaS Website upgrade. You can check the Management Agent version in the Control Panel of your external SQL virtual machine. If the Management Agent is not version 7.0 or later, complete these steps to upgrade the Management Agent.
  a. Open a browser and navigate to the VMware vRealize Automation IaaS Installation page on the Virtual Appliance appliance using the fully qualified domain name: https://virtual_appliance_host:5480/installer.
  b. Click **Management Agent Installer**.
     - By default, the installer is downloaded to the Downloads folder.
  c. Log in to the external database, upgrade the Management Agent with the Management Agent Installer file, and restart the Windows Management Agent service.
- If you have a Common Components Catalog component installed, you must uninstall the component before you upgrade. For more information, see the Common Components Catalog Installation Guide or follow the steps provided in Checklist for Upgrading vRealize Automation.
Procedure

1. If you are using a load balancer, prepare your environment.
   a. Verify the IaaS Website node that contains the Model Manager data is enabled for load balancer traffic.
      
      You can identify this node by the presence of the vCAC Folder\Server\ConfigTool folder.
   b. Disable all other IaaS Websites and non-primary Manager Services for load balancer traffic.

2. Right-click the setup__vrealize-automation-appliance-FQDN@5480.exe setup file and select Run as administrator.

3. Click Next.

4. Accept the license agreement and click Next.

5. Enter the administrator credentials for your current deployment on the Log In page.
   The user name is root and the password is the password that you entered when you deployed the appliance.


7. On the Installation Type page, verify that Upgrade is selected.
   If Upgrade is not selected, the components on this system are already upgraded to this version.

8. Click Next.

9. Configure the upgrade settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| If you are upgrading the Model Manager Data | Select the Model Manager Data check box in the vCAC Server section.  
The check box is selected by default. Upgrade the Model Manager data only once. When you upgrade a distributed installation, the Web servers stop functioning while there is a version mismatch between the Web servers and the Model Manager data. When the Model Manager data upgrade finishes, the Web servers function as usual.  |
| If you are not upgrading the Model Manager Data | Unselect the Model Manager Data check box in the vCAC Server section.  |
| To preserve customized workflows as the latest version in your Model Manager Data | If you are upgrading the Model Manager Data, select the Preserve my latest workflow versions check box in the Extensibility Workflows section.  
The check box is selected by default. Customized workflows are always preserved. Selecting the check box determines version order only. If you have customized workflows in the Model Manager, select this option to so that the most recent workflow remains as the most recent version after upgrade.  
If you do not select this option, the version of each workflow provided with vRealize Automation Designer becomes the most recent after upgrade. The most recent version before upgrade becomes the second most recent.  
For information about vRealize Automation Designer, see Life Cycle Extensibility.  |
| If you are upgrading a Distributed Execution Manager or a proxy agent | Enter the credentials for the administrator account in the Service Account section.  
All the services that you upgrade run under this account. |
To specify your Microsoft SQL Server database

If you upgrade the Model Manager Data, enter the names of the database server and database instance in the **Server** text box. Enter a fully qualified domain name (FQDN) for the database server name in the **Database name** text box.

If the database instance is on a non-default SQL port, include the port number in the server instance specification. The Microsoft SQL default port number is 1433.

When upgrading the manager nodes, the MSSQL SSL option is selected by default. If your database does not use SSL, deselect **Use SSL for database connection**.

---

10 Click **Next**.

11 Confirm that all services to upgrade appear on the Ready to Upgrade page, and click **Upgrade**.

The Upgrading page and a progress indicator appear. When the upgrade process finishes, the **Next** button is enabled.

12 Click **Next**.

13 Click **Finish**.

14 Verify that all services restarted.

15 Repeat these steps for each IaaS server in your deployment in the stated order.

16 After all components are upgraded, log in to the management console for the appliance and verify that all services, including IaaS, are now registered.

All the selected components are upgraded to the new release.

**What to do next**

- **Restore Access to Built-In vRealize Orchestrator Control Center**.

- If your deployment uses a load balancer, upgrade each load balancer node to use vRealize Automation health checks. Re-enable load balancer traffic for any unconnected nodes. If your previous deployment used a load balanced embedded PostgreSQL database, disable all nodes in the PostgreSQL pool because they are not needed. Delete the pool at a convenient time.

  For more information, see [vRealize Automation Load Balancing](#).

- (Optional) Enable automatic Manager Service failover. See [Enable Automatic Manager Service Failover After Upgrade](#).

**Restore Access to Built-In vRealize Orchestrator Control Center**

After you upgrade the IaaS server components, you must restore access to the vRealize Orchestrator.

When you upgrade vRealize Automation 6.2.5 to 7.4, you need to perform this procedure to accommodate the new Role-Based Access Control feature. This procedure is written for a high-availability environment.

**Prerequisites**

Make a snapshot of your vRealize Automation environment.
Procedure

1. Log in to the vRealize Automation appliance management console as root by using the appliance host fully qualified domain name, https://va-hostname.domain.name:5480.

2. Select vRA Settings > Database.

3. Identify the master and replica nodes.

4. On each replica node, open an SSH session, log in as administrator, and run this command:
   
   service vco-server stop && service vco-configurator stop

5. On the master node, open an SSH session, log in as administrator, and run this command:
   
   rm /etc/vco/app-server/vco-registration-id

6. On the master node, change directories to /etc/vco/app-server/.

7. Open the sso.properties file.

8. If the property name com.vmware.o11n.sso.admin.group.name contains spaces or any other Bash-related characters that can be accepted as a special character in a Bash command such as a hyphen (') or a dollar sign ($), complete these steps.
   
   a. Copy the line with the com.vmware.o11n.sso.admin.group.name property and enter AdminGroup for the value.
   
   b. Add # to the beginning of the original line with the com.vmware.o11n.sso.admin.group.name property to comment the line.
   
   c. Save and close the sso.properties file.

9. Run this command:
   
   vcac-vami vco-service-reconfigure

10. If you completed step 8, open the sso.properties file and complete these steps.

    a. Remove the # from the beginning of the original line with the com.vmware.o11n.sso.admin.group.name property to uncomment the line.

    b. Remove the copy of the line with the com.vmware.o11n.sso.admin.group.name property.

    c. Save and close the sso.properties file.

11. Run this command to restart the vco-server service:

    service vco-server restart

12. Run this command to restart the vco-configurator service:

    service vco-configurator restart

13. In the vRealize Automation appliance management console, click Services and wait until all the services in the master node are REGISTERED.
14 When all the services are registered, join the vRealize Automation replica nodes to the
vRealize Automation cluster to synchronize the vRealize Orchestrator configuration. For information,
see Reconfigure the Built-In vRealize Orchestrator to Support High Availability.

What to do next

Upgrading vRealize Orchestrator After Upgrading vRealize Automation.

Upgrading vRealize Orchestrator After Upgrading vRealize Automation

You must upgrade your vRealize Orchestrator instance after you upgrade from vRealize Automation 6.2.5
to 7.4.

With the release of vRealize Orchestrator 7.4, you have two options for upgrading vRealize Orchestrator
after a successful upgrade to vRealize Automation 7.4.

- You can migrate your existing external vRealize Orchestrator server to the embedded
  vRealize Orchestrator included in vRealize Automation 7.4.
- You can upgrade your existing standalone or clustered vRealize Orchestrator server to work with
  vRealize Automation 7.4.

Migrating an External vRealize Orchestrator Server to vRealize Automation

You can migrate your existing external vRealize Orchestrator server to a vRealize Orchestrator instance
embedded in vRealize Automation 7.4.

You can deploy vRealize Orchestrator as an external server instance and configure vRealize Automation
to work with that external instance, or you can configure and use the vRealize Orchestrator server that is
included in the vRealize Automation appliance.

VMware recommends that you migrate your external vRealize Orchestrator to the Orchestrator server that
is built into vRealize Automation. The migration from an external to embedded Orchestrator provides the
following benefits:

- Reduces the total cost of ownership.
- Simplifies the deployment model.
- Improves the operational efficiency.

Note Consider using the external vRealize Orchestrator in the following cases:

- Multiple tenants in the vRealize Automation environment
- Geographically dispersed environment
- Workload handling
- Use of specific plug-ins, such as older versions of the Site Recovery Manager plug-in

Control Center Differences Between External and Embedded Orchestrator

Some of the menu items that are available in Control Center of an external vRealize Orchestrator are not
included in the default Control Center view of an embedded Orchestrator instance.
In Control Center of the embedded Orchestrator server, a few options are hidden by default.

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.</td>
</tr>
<tr>
<td>Export/Import Configuration</td>
<td>The embedded Orchestrator configuration is included in the exported vRealize Automation components.</td>
</tr>
<tr>
<td>Configure Database</td>
<td>The embedded Orchestrator uses the database that is used by vRealize Automation.</td>
</tr>
</tbody>
</table>
| Customer Experience Improvement Program | You can join the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance management interface.  
  See The Customer Experience Improvement Program in Managing vRealize Automation. |

Another options that are hidden from the default Control Center view are the Host address text box and the UNREGISTER button on the Configure Authentication Provider page.

**Note** To see the full set of Control Center options in vRealize Orchestrator that is built into vRealize Automation, you must access the advanced Orchestrator Management page at https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/?advanced and click the F5 button on the keyboard to refresh the page.

**Migrate an External vRealize Orchestrator on Windows to vRealize Automation**

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x installed on Windows to the Orchestrator server that is built into vRealize Automation 7.4.

**Note** If you have a distributed vRealize Automation environment with multiple vRealize Automation nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**
- Successful migration to vRealize Automation 7.4.
- Stop the Orchestrator server service on the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

**Procedure**

1. Download the migration tool from the target Orchestrator server.
   a. Log in to the vRealize Automation appliance over SSH as root.
   b. Download the migration-tool.zip archive that is located in the /var/lib/vco/downloads directory.

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. Set the PATH environment variable by pointing it to the bin folder of the Java JRE installed with Orchestrator.
   b. Upload the migration tool to the Windows server, on which the external Orchestrator is installed.
c Extract the downloaded archive in the Orchestrator install folder. The default path to the Orchestrator install folder in a Windows-based installation is `C:\Program Files\VMware\Orchestrator`.

d Run the Windows command prompt as administrator and navigate to the `bin` folder in the Orchestrator install folder. By default, the path to the `bin` folder is `C:\Program Files\VMware\Orchestrator\migration-cli\bin`.

e Run the export command from the command line.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

This command combines the vRealize Orchestrator configuration files and plug-ins into an export archive. The archive is created in the same folder as the `migration-cli` folder.

3 Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.

a Upload the exported configuration file to the `/usr/lib/vco/tools/configuration-cli/bin` directory on the vRealize Automation appliance.

b Under the `/usr/lib/vco/tools/configuration-cli/bin` directory, change the ownership of the exported Orchestrator configuration file.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

c Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```
Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the db-migrate command.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Note**  Enclose passwords that contain special characters in single quotation marks.

The **JDBC_connection_URL** depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port:database_name`

The default database login information is:

<table>
<thead>
<tr>
<th>database_name</th>
<th>vmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>database_user</td>
<td>vmware</td>
</tr>
<tr>
<td>database_user_password</td>
<td>vmware</td>
</tr>
</tbody>
</table>

5 If you migrated vRealize Automation instead of upgrading it, delete the trusted Single Sign-On certificates from the database of the embedded Orchestrator instance.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

You successfully migrated an external vRealize Orchestrator 6.x installed on Windows to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

**What to do next**

Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

**Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4**

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x Virtual Appliance to the Orchestrator server that is built into vRealize Automation 7.4.

**Note**  If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.
Prerequisites

- Successful migration to vRealize Automation 7.4.
- Stop the Orchestrator server service on the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1. Download the migration tool from the target Orchestrator server to the source Orchestrator.
   a. Log in to the vRealize Orchestrator 6.x Virtual Appliance over SSH as root.
   b. Under the /var/lib/vco directory, run the scp command to download the migration-tool.zip archive.
      ```
      scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
      ```
   c. Run the unzip command to extract the migration tool archive.
      ```
      unzip migration-tool.zip
      ```

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. In the /var/lib/vco/migration-cli/bin directory, run the export command.
      ```
      ./vro-migrate.sh export
      ```
   This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.
   An archive with file name orchestrator-config-export-orchestrator_ip_address-date_hour.zip is created in the /var/lib/vco folder.

3. Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.
   a. Log in to the vRealize Automation appliance over SSH as root.
   b. Under the /usr/lib/vco/tools/configuration-cli/bin directory, run the scp command to download the exported configuration archive.
      ```
      scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
      ```
   c. Change the ownership of the exported Orchestrator configuration file.
      ```
      chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
      ```
d Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

```
service vco-server stop & service vco-configurator stop
```

e Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the import command.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --notSkipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

4 If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.

a In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.

b Set the values of `listen_addresses` to a wildcard (`*`).

```
listen_addresses ='*'
```

c Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.

```
host all all vra-va-ip-address/32 md5
```

**Note** The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.

d Restart the PostgreSQL server service.

```
service vpostgres restart
```
5 Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the db-migrate command.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Note** Enclose passwords that contain special characters in single quotation marks.

The **JDBC_connection_URL** depends on the type of database that you use.

- **PostgreSQL**: `jdbc:postgresql://host:port/database_name`
- **Oracle**: `jdbc:oracle:thin:@host:port:database_name`

The default database login information is:

<table>
<thead>
<tr>
<th><code>database_name</code></th>
<th><code>vmware</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>

6 If you migrated vRealize Automation instead of upgrading it, delete the trusted Single Sign-On certificates from the database of the embedded Orchestrator instance.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

7 Revert to the default configuration of the `postgresql.conf` and the `pg_hba.conf` file.

- a Restart the PostgreSQL server service.

You successfully migrated an external vRealize Orchestrator 6.x Virtual Appliance to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

**What to do next**

Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

**Configure the Built-In vRealize Orchestrator Server**

After you export the configuration of an external Orchestrator server and import it to vRealize Automation 7.4, you must configure the Orchestrator server that is built into vRealize Automation.

**Prerequisites**

Migrate the configuration from the external to the internal vRealize Orchestrator.
Procedure

1. Log in to the vRealize Automation appliance over SSH as root.

2. Start the Control Center service and the Orchestrator server service of the built-in vRealize Orchestrator server.

   ```
service vco-configurator start && service vco-server start
   ```

3. Log in to Control Center of the built-in Orchestrator server as an administrator.

   **Note** If you migrate from an external vRealize Orchestrator 7.4 instance, skip to step 5.

4. Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

5. If the external Orchestrator was configured to work in cluster mode, reconfigure the Orchestrator cluster in vRealize Automation.

      **Note** If the Remove check boxes next the existing nodes in the cluster do not appear, you must refresh the browser page by clicking the F5 button on the keyboard.

   b. Select the check boxes next to the external Orchestrator nodes and click Remove to remove them from the cluster.

   c. To exit the advanced cluster management page, delete the remove-nodes string from the URL and refresh the browser page by clicking the F5 button on the keyboard.

   d. At the Validate Configuration page in Control Center, verify that Orchestrator is configured properly.


7. (Optional) Change the values for Default tenant and Admin group on the Configure Authentication Provider page.

8. Verify that the vco-server service appears as REGISTERED under the Services tab in the vRealize Automation appliance management console.

9. Select the vco services of the external Orchestrator server and click Unregister.

What to do next

- Import any certificates that were trusted in the external Orchestrator server to the trust store of the built-in Orchestrator.

- Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the Orchestrator configuration.
For more information, see Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability in Installing or Upgrading vRealize Automation.

**Note** The vRealize Orchestrator instances are automatically clustered and available for use.

- Restart the vco-configurator service on all nodes in the cluster.
- Update the vRealize Orchestrator endpoint to point to the migrated built-in Orchestrator server.
- Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.

### Upgrading Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation

If you maintain a stand-alone vRealize Orchestrator appliance for use with vRealize Automation, you must upgrade the stand-alone appliance when you upgrade vRealize Automation from 6.2.5 to 7.4. Embedded instances of vRealize Orchestrator are upgraded as part of the vRealize Automation appliance upgrade. No additional action is required for an embedded instance.

If you are upgrading a vRealize Orchestrator appliance cluster, see Upgrading External vRealize Orchestrator Appliance Cluster for Use with vRealize Automation.

**Prerequisites**

- Install the Update on the vRealize Automation Appliance.
- Upgrade IaaS components as described in Upgrading the IaaS Server Components After Upgrading vRealize Automation.
-Unmount all network file systems. See *vSphere Virtual Machine Administration* in the vSphere documentation.
-Increase the memory of the vSphere Orchestrator appliance to at least 6 GB. See *vSphere Virtual Machine Administration* in the vSphere documentation.
-Take a snapshot of the vSphere Orchestrator virtual machine. See *vSphere Virtual Machine Administration* in the vSphere documentation.
-If you use an external database, back up the database.
-If you use the preconfigured PostgreSQL database in vSphere Orchestrator, back up the database by using the **Export Database** menu in the vSphere Control Center.

**Procedure**

1. Use one of the documented methods to upgrade your stand-alone vRealize Orchestrator.
   - Upgrade Orchestrator Appliance by Using the Default VMware Repository.
   - Upgrade Orchestrator Appliance by Using an ISO Image.
   - Upgrade Orchestrator Appliance by Using a Specified Repository.
2. From the Control Center, upgrade the vRealize Automation NSX plugin.
Upgrade Orchestrator Appliance by Using the Default VMware Repository

You can configure Orchestrator to download the upgrade package from the default VMware repository.

**Prerequisites**

- Unmount all network file systems. For more information, see the *vSphere Virtual Machine Administration* documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the *vSphere Virtual Machine Administration* documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
- Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.
- Take a snapshot of the Orchestrator virtual machine. For more information, see the *vSphere Virtual Machine Administration* documentation.
- If you use an external database, back up the database.
- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

**Procedure**

1. Go to the Virtual Appliance Management Interface (VAMI) at https://orchestrator_server:5480 and log in as root.
2. On the Update tab, click Settings. The radio button next to the Use Default Repository option is selected.
3. On the Status page, click Check Updates.
4. If any updates are available, click Install Updates.
5. Accept the VMware End-User License Agreement and confirm that you want to install the update.
6. To complete the update, restart the Orchestrator Appliance.
   a. Log in again to the to the Virtual Appliance Management Interface (VAMI) as root.
7. (Optional) On the Update tab, verify that the latest version of the Orchestrator Appliance is successfully installed.
8. Log in to Control Center as root.
9. If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.
   a. On the Host Settings page in Control Center, click CHANGE.
   b. Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.
10 Reconfigure the authentication.

a If before the upgrade, the Orchestrator server was configured to use LDAP or SSO (legacy) as an authentication method, configure vSphere or vRealize Automation as an authentication provider.

b If the authentication is already set to vSphere or vRealize Automation, unregister the settings and register them again.

**Note** If before the upgrade, your Orchestrator used vSphere as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.

You successfully upgraded the Orchestrator Appliance.

**What to do next**

Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

**Upgrade Orchestrator Appliance by Using an ISO Image**

You can configure Orchestrator to download the upgrade package from an ISO image file mounted to the CD-ROM drive of the appliance.

**Prerequisites**

- Unmount all network file systems. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
- Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.
- Take a snapshot of the Orchestrator virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.
- If you use an external database, back up the database.
- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

**Procedure**

1 Download the VMware-vRO-Appliance-version-build_number-updaterepo.iso archive from the official VMware download site.
2 Connect the CD-ROM drive of the Orchestrator Appliance virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.

3 Mount the ISO image file to the CD-ROM drive of the appliance. For more information, see the vSphere Virtual Machine Administration documentation.

4 Go to the Virtual Appliance Management Interface (VAMI) at https://orchestrator_server:5480 and log in as root.

5 On the Update tab, click Settings.

6 Select the radio button next to the Use CD-ROM updates option.

7 Return to the Status page.

   The version of the available upgrade is displayed.

8 Click Install Updates.

9 Accept the VMware End-User License Agreement and confirm that you want to install the update.

10 To complete the update, restart the Orchestrator Appliance.

   a Log in again to the to the Virtual Appliance Management Interface (VAMI) as root.

11 (Optional) On the Update tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

12 Log in to Control Center as root.

13 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.

   a On the Host Settings page in Control Center, click CHANGE.

   b Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

14 Reconfigure the authentication.

   a If before the upgrade, the Orchestrator server was configured to use LDAP or SSO (legacy) as an authentication method, configure vSphere or vRealize Automation as an authentication provider.

   b If the authentication is already set to vSphere or vRealize Automation, unregister the settings and register them again.

   Note  If before the upgrade, your Orchestrator used vSphere as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.

You successfully upgraded the Orchestrator Appliance.
What to do next

Verify that Orchestrator is configured properly at the Validate Configuration page in Control Center.

Upgrade Orchestrator Appliance by Using a Specified Repository

You can configure Orchestrator to use a local repository, on which you uploaded the upgrade archive.

Prerequisites

- Unmount all network file systems. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the vSphere Virtual Machine Administration documentation.
- Increase the vRealize Orchestrator virtual machine disk size: Disk1=7 GB, Disk2=10 GB.
- Make sure that the root partition of the Orchestrator Appliance has at least 1 GB of available free space. For more information on increasing the size of a disk partition, see KB 57345: https://kb.vmware.com/s/article/57345.
- Take a snapshot of the Orchestrator virtual machine. For more information, see the vSphere Virtual Machine Administration documentation.
- If you use an external database, back up the database.
- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the Export Database menu in Control Center.

Procedure

1. Prepare the local repository for upgrades.
   a. Install and configure a local Web server.
   b. Download the VMware-vRO-Appliance-version-build_number-updaterrepo.zip archive from the official VMware download site.
   c. Extract the .ZIP archive to the local repository.
2. Go to the Virtual Appliance Management Interface (VAMI) at https://orchestrator_server:5480 and log in as root.
3. On the Update tab, click Settings.
4. Select the radio button next to the Use Specified Repository option.
5. Enter the URL address of the local repository by pointing to the Update_Repo directory.
   

6. If the local repository requires authentication, enter user name and password.
7. Click Save Settings.
8. On the Status page, click Check Updates.
9 If any updates are available, click **Install Updates**.

10 Accept the VMware End-User License Agreement and confirm that you want to install the update.

11 To complete the update, restart the Orchestrator Appliance.
   a Log in again to the Virtual Appliance Management Interface (VAMI) as **root**.

12 (Optional) On the **Update** tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

13 Log in to Control Center as **root**.

14 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.
   a On the **Host Settings** page in Control Center, click **CHANGE**.
   b Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

15 Reconfigure the authentication.
   a If before the upgrade, the Orchestrator server was configured to use **LDAP** or **SSO (legacy)** as an authentication method, configure **vSphere** or **vRealize Automation** as an authentication provider.
   b If the authentication is already set to **vSphere** or **vRealize Automation**, unregister the settings and register them again.

**Note** If before the upgrade, your Orchestrator used **vSphere** as an authentication provider and was configured to connect to the vCenter Server fully qualified domain name or IP address, in case you have an external Platform Services Controller, after the upgrade you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On. You must also import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain.

You successfully upgraded the Orchestrator Appliance.

**What to do next**

Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

**Upgrading External vRealize Orchestrator Appliance Cluster for Use with vRealize Automation**

If you use an vRealize Orchestrator appliance cluster with vRealize Automation, you must upgrade the Orchestrator appliance cluster to version 7.4 by upgrading a single instance and joining newly installed 7.4 nodes to the upgraded instance.

**Prerequisites**

- Install the Update on the vRealize Automation Appliance.
- Upgrade IaaS components. See Upgrading the IaaS Server Components After Upgrading vRealize Automation.
- Set up a load balancer to distribute traffic among multiple instances of vRealize Orchestrator. See the vRealize Orchestrator Load Balancing Configuration Guide.
- Take a snapshot of all vRealize Orchestrator server nodes.
- Back up the vRealize Orchestrator shared database.

**Procedure**

1. From the Control Center, upgrade the vRealize Automation NSX plugin.
2. Stop the `vco-server` and `vco-configurator` Orchestrator services on all cluster nodes.
3. Upgrade only one of the Orchestrator server instances in your cluster using one of the documented procedures.
4. Deploy a new Orchestrator appliance on version 7.4.
   a. Configure the new node with the network settings of an existing not upgraded instance that is part of the cluster.
5. Access Control Center of the second node to start the configuration wizard.
   b. Log in as root with the password you entered during OVA deployment.
6. Select the **Clustered Orchestrator** deployment type.
   By choosing this type, you select to join the node to an existing Orchestrator cluster.
7. In the **Hostname** text box, enter the host name or IP address of the first Orchestrator server instance.
   
   **Note** This must be the local IP or host name of the Orchestrator instance, to which you are joining the second node. You must not use the load balancer address.
8. In the **User name** and **Password** text boxes, enter the root credentials of the first Orchestrator server instance.
9. Click **Join**. The Orchestrator instance clones the configuration of the node, to which it joins.
   The Orchestrator server service of both nodes restart automatically.
10. Access Control Center of the upgraded Orchestrator cluster through the load balancer address and log in as an **administrator**.
11. On the **Orchestrator Cluster Management** page, make sure that the **Active Configuration Fingerprint** and the **Pending Configuration Fingerprint** strings on all nodes in the cluster match.
   
   **Note** You might need to refresh the page several times until the two strings match.
12. Verify that the vRealize Orchestrator cluster is configured properly by opening the **Validate Configuration** page in Control Center.
13 (Optional) Repeat steps 3 through 8 for each additional node in the cluster.

14 From the Control Center, upgrade the vRealize Automation NSX plugin.

You have successfully upgraded the Orchestrator cluster.

**What to do next**

Enable Your Load Balancers.

**Add Users or Groups to an Active Directory Connection**

You can add users or groups to an existing Active Directory connection.

The Directories Management user authentication system imports data from Active Directory when adding groups and users. The speed of the data transport is limited by Active Directory capabilities. As a result, actions can take a long time depending on the number of groups and users that are added. To minimize problems, limit the groups and users to only the groups and users required for a vRealize Automation action. If problems occur, close unneeded applications and verify that your deployment has appropriate memory allocated to Active Directory. If problems continue, increase the Active Directory memory allocation. For deployments with large numbers of users and groups, you might need to increase the Active Directory memory allocation to as much as 24 GB.

When you sync a vRealize Automation deployment with a many users and groups, there might be a delay before the SyncLog details are available. The time stamp on the log file can differ from the completed time displayed on the console.

If members of a group are not in the Users list, when you add the group from Active Directory, the members are added to the list. When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.

**Note** You cannot cancel a synchronize action after you start the action.

**Prerequisites**

- Connector installed and the activation code activated. Select the required default attributes and add additional attributes on the User Attributes page.
- List of the Active Directory groups and users to sync from Active Directory.
- For Active Directory over LDAP, information required includes the Base DN, Bind DN, and Bind DN password.
- For Active Directory Integrated Windows Authentication, the information required includes the domain's Bind user UPN address and password.
- If Active Directory is accessed over SSL, a copy of the SSL certificate is required.
- If you have a multi-forest Active Directory integrated with Windows Authentication and the Domain Local group contains members from different forests, do the following. Add the Bind user to the Administrators group of the Domain Local group. If the Bind user is not added, these members are missing from the Domain Local group.
Log in to vRealize Automation as a tenant administrator.

Procedure
1. Select **Administration > Directories Management > Directories**.
2. Click the desired directory name.
3. Click **Sync Settings** to open a dialog box with synchronization options.
4. Click the appropriate icon depending on whether you want to change the user or group configuration.
   To edit the group configuration:
   - To add groups, click the + icon to add a line for group DN definitions and enter the appropriate group DN.
   - If you want to delete a group DN definition, click the x icon for the desired group DN.
   To edit the user configuration:
   - To add users, click the + icon to add a line for a user DN definition and enter the appropriate user DN.
   - If you want to delete a user DN definition, click the x icon for the desired user DN.
5. Click **Save** to save your changes without synchronizing your updates immediately. Click **Save & Sync** to save your changes and synchronize your updates immediately.

Enable Your Load Balancers
If your deployment uses load balancers, re-enable secondary nodes and health checks and revert the load balancer timeout settings.

The health checks for vRealize Automation vary according to version. For information, see the vRealize Automation Load Balancing Configuration Guide in the VMware vRealize Automation Documentation.

Change the load balancer timeout settings from 10 minutes back to the default.

Post-Upgrade Tasks for Upgrading vRealize Automation
After you upgrade vRealize Automation 6.2.5 to 7.4, perform any required post-upgrade tasks.

Port Configuration for High-Availability Deployments
After finishing an upgrade in a high-availability deployment, you must configure the load balancer to pass traffic on port 8444 to the vRealize Automation appliance to support remote console features.

For more information, see the vRealize Automation Load Balancing Configuration Guide in the vRealize Automation Documentation.

Reconfigure the Built-In vRealize Orchestrator to Support High Availability
For a high-availability deployment, you must manually rejoin each target replica vRealize Automation appliance to the cluster to enable high-availability support for the embedded vRealize Orchestrator.
Prerequisites

Log in to the target replica vRealize Automation appliance management console.

1 Start a browser and open the target replica vRealize Automation management console using the fully qualified domain name (FQDN) of the target replica virtual appliance: https://vra-va-hostname.domain.name:5480.

2 Log in with the user name root and the password that you entered when you deployed the target replica vRealize Automation appliance.

Procedure

1 Select vRA Settings > Cluster.

2 In the Leading Cluster Node text box, enter the FQDN of the target master vRealize Automation appliance.

3 Enter the root password in the Password text box.

4 Click Join Cluster.

   Continue past any certificate warnings. The system restarts services for the cluster.

5 Verify that the services are running.
   a On the top tab bar, click Services.
   b Click Refresh to monitor the progress of services startup.

Enabling the Connect to Remote Console Action for Consumers

The remote console action for consumers is supported for appliances provisioned by vSphere in vRealize Automation.

Edit the blueprint after you have upgraded the release and select the Connect to Remote Console action on the Action tab.

For more information, see Knowledge Base article 2109706.

Restore External Workflow Timeout Files

You must reconfigure the vRealize Automation external workflow timeout files because the upgrade process overwrites xmldb files.

Procedure

1 Open the external workflow configuration (xmldb) files on your system from the following directory. \VMware\vCAC\Server\ExternalWorkflows\xmldb\.

2 Replace the xmldb files with the files that you backed up before migration. If you do not have backup files, reconfigure the external workflow timeout settings.

3 Save your settings.
Verify That vRealize Orchestrator Service Is Available

After you upgrade to the latest version of vRealize Automation, you must verify the connection between vRealize Automation and vRealize Orchestrator. Sometimes after upgrade you must restore the connection.

Prerequisites

Log in to the vRealize Orchestrator configuration interface.

Procedure

1. Click Validate Configuration.
2. If the Authentication section has a green check, go to step 5.
3. If the Authentication section does not have a green check, perform the following steps to restore the connection to vRealize Orchestrator:
   a. Click Home.
   b. Click Configure Authentication Provider.
   c. In the Admin group text box, select Change, and choose a new Admin group that can be properly resolved.
      The vcoadmins group is available only at the default vsphere.local tenant. If you are using another tenant for the vRealize Orchestrator, then you must select another group.
   d. Click Save Changes, and if prompted, restart the vRealize Orchestrator server.
   e. Click Home.
4. Repeat step 1 to confirm that the Authentication section still has a green check.
5. Click Home, and close the vRealize Orchestrator Control Center.

Reconfigure Embedded vRealize Orchestrator Infrastructure Endpoint in the Target vRealize Automation

When you migrate from a vRealize Automation 6.2.x environment, you must update the URL of the infrastructure endpoint that points to the target embedded vRealize Orchestrator server.

Prerequisites

- Successfully migrate to vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.
     For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.
  b. Log in as a IaaS administrator user.
Procedure

1. Select Infrastructure > Endpoints > Endpoints.

2. On the Endpoints page, select the vRealize Orchestrator endpoint, and click Edit.

3. In the Address text box, edit the vRealize Orchestrator endpoint URL.
   - If you migrated to a minimal environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-hostname.domain.name:443/vco.
   - If you migrated to a high-availability environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-lb-hostname.domain.name:443/vco.

4. Click OK.

5. Manually run a data collection on the vRealize Orchestrator endpoint.
   a. On the Endpoints page, select the vRealize Orchestrator endpoint.
   b. Select Actions > Data Collection.
      Verify that the data collection is successful.

Restore Changes to Logging in the app.config File

The upgrade process overwrites changes you make to logging in the configuration files. After you finish an upgrade, you must restore any changes you made before the upgrade to the app.config file.

Enable Automatic Manager Service Failover After Upgrade

Automatic Manager Service failover is disabled by default when you upgrade vRealize Automation.

Complete these steps to enable automatic Manager Service after upgrade.

Procedure

1. Open a command prompt as root on the vRealize Automation appliance.


3. To enable automatic Manager Service failover, run the following command.
   python ./manager-service-automatic-failover ENABLE
   To disable automatic failover throughout an IaaS deployment, run the following command.
   python ./manager-service-automatic-failover DISABLE

About Automatic Manager Service Failover

You can configure the vRealize Automation IaaS Manager Service to automatically fail over to a backup if the primary Manager Service stops.

Starting in vRealize Automation 7.3, you no longer need to manually start or stop the Manager Service on each Windows server, to control which serves as primary or backup. Automatic Manager Service failover is disabled by default when you upgrade IaaS with the Upgrade Shell Script or using the IaaS Installer executable file.
When automatic failover is enabled, the Manager Service automatically starts on all Manager Service hosts, including backups. The automatic failover feature allows the hosts to transparently monitor each other and fail over when necessary, but the Windows service must be running on all hosts.

**Note** You are not required to use automatic failover. You may disable it and continue to manually start and stop the Windows service to control which host serves as primary or backup. If you take the manual failover approach, you must only start the service on one host at a time. With automatic failover disabled, simultaneously running the service on multiple IaaS servers makes vRealize Automation unusable.

Do not attempt to selectively enable or disable automatic failover. Automatic failover must always be synchronized as on or off, across every Manager Service host in an IaaS deployment.

**Run Test Connection and Verify Upgraded Endpoints**

Upgrading from vRealize Automation 7.3 or earlier to 7.4 makes changes to endpoints in the target environment.

After you upgrade to vRealize Automation 7.4, you must use the **Test Connection** action for all applicable endpoints. You might also need to make adjustments to some upgraded endpoints. For more information, see Considerations When Working With Upgraded or Migrated Endpoints.

The default security setting for upgraded or migrated endpoints is not to accept untrusted certificates.

After upgrading or migrating from an earlier vRealize Automation installation, if you were using untrusted certificates you must perform the following steps for all vSphere and NSX endpoints to enable certificate validation. Otherwise, the endpoint operations fail with certificate errors. For more information, see VMware Knowledge Base articles *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* at http://kb.vmware.com/kb/2150230 and *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* at http://kb.vmware.com/kb/2108294.

1. After upgrade or migration, log in to the vRealize Automation vSphere agent machine and restart your vSphere agents by using the **Services** tab.
   
   Migration might not restart all agents, so manually restart them if needed.

2. Wait for at least one ping report to finish. It takes a minute or two for a ping report to finish.

3. When the vSphere agents have started data collection, log in to vRealize Automation as an IaaS administrator.

4. Click **Infrastructure > Endpoints > Endpoints**.

5. Edit a vSphere endpoint and click **Test Connection**.

6. If a certificate prompt appears, click **OK** to accept the certificate.

   If a certificate prompt does not appear, the certificate might currently be correctly stored in a trusted root authority of the Windows machine hosting service for the endpoint, for example as a proxy agent machine or DEM machine.

7. Click **OK** to apply the certificate acceptance and save the endpoint.

8. Repeat this procedure for each vSphere endpoint.
9 Repeat this procedure for each NSX endpoint.

If the Test Connection action is successful but some data collection or provisioning operations fail, you can install the same certificate on all the agent machines that serve the endpoint and on all DEM machines. Alternatively, you can uninstall the certificate from existing machines and repeat the preceding procedure for the failing endpoint.

**Import DynamicTypes**

If you are using the DynamicTypes plug-in, and you exported the configuration as a package before the upgrade, you must import the following workflow.

1 Import Dynamic Types Configuration in the target environment.
   a Log in to the Java Client as administrator.
   b Select the Workflows tab.
   c Select Library > Dynamic Types > Configuration.
   d Select the Import Configuration From Package workflow and run it.
   e Click Configuration package to import.
   f Browse to the exported package file and click Attach file.
   g Review the information about the namespaces attached to the package and click Submit

2 Select Inventory > Dynamic Types to verify that the dynamic type namespaces have been imported.

**Troubleshooting the vRealize Automation Upgrade**

The upgrade troubleshooting topics provide solutions to problems that you might encounter when upgrading vRealize Automation 6.2.5 to 7.4.

**Installation or Upgrade Fails with a Load Balancer Timeout Error**

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

**Problem**

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.

**Cause**

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

**Solution**

1 Increase your load balancer timeout value to at least 100 seconds.
2 Rerun the installation or upgrade.
Upgrade Fails for IaaS Website Component

The IaaS upgrade fails and you cannot continue the upgrade.

Problem

The IaaS upgrade fails for the website component. The following error messages appear in the installer log file.

- System.Data.Services.Client.DataServiceQueryException:
  An error occurred while processing this request. --->
- <b>Description:</b> An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.
- Done Building Project "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"
  (InstallRepoModel target(s)) -- FAILED.

The following error messages appear in the repository log file.

- [Error]: [sub-thread-id="20"
  context="" token=""] Failed to start repository service. Reason:
  System.InvalidOperationException: Configuration section encryptionKey is not protected
  at
  DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration config)
  at

IaaS upgrade fails when the creation date for the `web.config` file is the same as or later than the modified date.

**Solution**

1. On the IaaS host, log in to Windows.
2. Open the Windows command prompt.
3. Change directories to the vRealize Automation installation folder.
4. Start your preferred text editor with the **Run as Administrator** option.
5. Locate and select the `web.config` file and save the file to change its file modification date.
6. Examine the `web.config` file properties to confirm that the file modification date is later than the creation date.
7. Upgrade IaaS.

**Manager Service Fails to Run Due to SSL Validation Errors During Runtime**

The manager service fails to run due to SSL validation errors.

**Problem**

The manager service fails with the following error message in the log:

```
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable `1 source)
at DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String coreModelConnectionString)
```
[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core database, will retry in 00:00:05, error details: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)

**Cause**

During runtime, the manager service fails to run due to SSL validation errors.

**Solution**

1. Open the `ManagerService.config` configuration file.
2. Update `Encrypt=False` on the following line:

   ```xml
   <add name="vcac-repository" providerName="System.Data.SqlClient"
    connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
   ```

**Log In Fails After Upgrade**

You must exit the browser and log in again after an upgrade for sessions that use unsynchronized user accounts.

**Problem**

After you upgrade vRealize Automation, the system denies access to unsynchronized user accounts at login.

**Solution**

Exit the browser and relaunch vRealize Automation.

**Catalog Items Appear in the Service Catalog After Upgrade But Are Not Available to Request**

Catalog items that use certain property definitions from prior versions appear in the service catalog but are not available to request after upgrading to the latest version of vRealize Automation.

**Problem**

If you upgraded from a 6.2.x or earlier version and you had property definitions with the following control types or attributes, the attributes are missing from the property definitions and any catalog items that use the definitions do not function the way that they did before you performed the upgrade.

- **Control types.** Check box or link.
- **Attributes.** Relationship, regular expressions, or property layouts.
Cause

In vRealize Automation 7.0 and later, the property definitions no longer use the attributes. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes.

Migrate the control type or attributes to vRealize Automation 7.x using a script action.

Solution

1. In vRealize Orchestrator, create a script action that returns the property values. The action must return a simple type. For example, return strings, integers, or other supported types. The action can take the other properties on which it depends as an input parameter.

2. In vRealize Automation console, configure the product definition.
   b. Select the property definition and click Edit.
   c. From the Display advice drop-down menu, select Dropdown.
   d. From the Values drop-down menu, select External Values.
   e. Select the script action.
   f. Click OK.
   g. Configure the Input Parameters that are included in the script action. To preserve the existing relationship, bind the parameter to the other property.
   h. Click OK.

PostgreSQL External Database Merge Is Unsuccessful

The external PostgreSQL database merge with the embedded PostgreSQL database does not succeed.

Problem

If the external PostgreSQL database version is newer than the embedded PostgreSQL database version, the merge does not succeed.

Solution

1. Log in to the host for the PostgreSQL external database.
2. Run the psql --version command.
   Note the PostgreSQL version for the external database.
3. Log in to the host for the PostgreSQL embedded database.
4. Run the psql --version command.
   Note the PostgreSQL version for the embedded database.

If the external PostgreSQL version is newer than the embedded PostgreSQL version, contact support for assistance to merge your external PostgreSQL database.
Join Cluster Command Appears to Fail After Upgrading a High-Availability Environment

After you click Join Cluster in the management console on a secondary cluster node, the progress indicator disappears.

Problem

When you use the vRealize Automation appliance management console after upgrade to join a secondary cluster node to the primary node, the progress indicator disappears and no error or success message appears. This behavior is an intermittent problem.

Cause

The progress indicator disappears because some browsers stop waiting for a response from the server. This behavior does not stop the join cluster process. You can confirm that the join cluster process is successful by viewing the log file at /var/log/vmware/vcac/vcac-config.log.

Upgrade Is Unsuccessful if Root Partition Does Not Provide Sufficient Free Space

If sufficient free space is unavailable on the root partition of the vRealize Automation appliance host, upgrade cannot proceed.

Solution

This procedure increases the free space on the Disk 1 root partition of the vRealize Automation appliance host. In a distributed deployment, perform this procedure to increase the free space on each replica node sequentially, and then increase the free space on the master node.

Note When you perform this procedure, you might see the following warning messages:

- WARNING: Re-reading the partition table failed with error 16: Device or resource busy. The kernel still uses the old table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8) Syncing disks.

- Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel of the change, probably because it/they are in use. As a result, the old partition(s) will remain in use. You should reboot now before making further changes.

Ignore the message You should reboot now before making further changes. If you reboot your system before step 10, you corrupt the upgrade process.

Procedure

1. Power on the vRealize Automation appliance host virtual machine and log in as with a secure shell connection as the root user.
2 Run the following commands to stop services.
   a  service vcac-server stop
   b  service vco-server stop
   c  service vpostgres stop

3 Run the following command to unmount the swap partition.
   swapoff -a

4 Run the following command to delete the existing Disk 1 partitions and create a 44-GB root partition and a 6-GB swap partition.
   (echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo ' +44G';
    echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda

5 Run the following command to change the swap partition type.
   (echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda

6 Run the following command to set the Disk 1 bootable flag.
   (echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda

7 Run the following command to register the partition changes with the Linux kernel.
   partprobe
   If you see a message prompting you to reboot before you make further changes, ignore the message. Rebooting the system before step 10 corrupts the upgrade process.

8 Run the following command to format the new swap partition.
   mkswap /dev/sda2

9 Run the following command to mount the swap partition.
   swapon -a

10 Reboot the vRealize Automation appliance.

11 After the appliance reboots, run the following command to resize the Disk 1 partition table.
   resize2fs /dev/sda1

12 To verify that the disk expansion is successful, run df -h and check that the available disk space on /dev/sda1 is greater than 30 GB.

Backup Copies of .xml Files Cause the System to Time Out

vRealize Automation registers any file with an .xml extension in the \VMware\vCAC\Server\ExternalWorkflows\xmlldb\ directory. If this directory contains backup files with an .xml extension, the system runs duplicate workflows that cause the system to time out.
Solution

Workaround: When you back up files in this directory, move the backups to another directory, or change the extension of the backup file name to something other than .xml.

Delete Orphaned Nodes on vRealize Automation

An orphaned node is a duplicate node that is reported on the host but does not exist on the host.

Problem

When you verify that each IaaS and virtual appliance node is in a healthy state, you might discover that a host has one or more orphaned nodes. You must delete all orphaned nodes.

Solution

1. On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.
2. Select vRA settings > Cluster.
3. For each orphaned node in the table, click Delete.

Unable to Create New Directory in vRealize Automation

Trying to add new directory with the first sync connector fails.

Problem

This issue occurs due to a bad config-state.json file located in /usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/.

For information about fixing this issue, see Knowledge Base Article 2145438.

Some Virtual Machines Do Not Have a Deployment Created During Upgrade

Virtual machines in the missing state at the time of upgrade do not have a corresponding deployment created in the target environment.

Problem

If a virtual machine is in the missing state in the source environment during upgrade, a corresponding deployment is not created in the target environment. If a virtual machine goes out of the missing state after upgrade, you can import the machine to the target deployment using bulk import.

Certificate Not Trusted Error

When you view the infrastructure Log Viewer page in the vRealize Automation appliance console, you might see an endpoint connection failure report with these words, Certificate is not trusted.

Problem

On the vRealize Automation appliance console, select Infrastructure > Monitoring > Log. On the Log Viewer page, you might see a report similar to this:
Failed to connect to the endpoint. To validate that a secure connection can be established to this endpoint, go to the vSphere endpoint on the Endpoints page and click the Test Connection button.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Cause

Upgrading from vRealize Automation 7.3 or earlier to 7.4 makes changes to the endpoints from your original environment. For environments recently upgraded to vRealize Automation 7.4, the IaaS administrator must review each existing endpoint that uses a secure, https, connection. If an endpoint has a Certificate is not trusted error, the endpoint does not work properly.

Solution

1. Log in to the vRealize Automation console as an infrastructure administrator.
2. Select Infrastructure > Endpoints > Endpoints.
3. Complete these steps for each endpoint with a secure connection.
   a. Click Edit.
   b. Click Test Connection.
   c. Review the certificate details and click OK if you trust this certificate.
   d. Restart the Windows services for all IaaS Proxy Agents used by this endpoint.
4. Verify that Certificate is not trusted errors no longer appear on the infrastructure Log Viewer page.

Installing or Upgrading to vRealize Automation Fails While Applying Prerequisite Fixes

Installing or upgrading vRealize Automation fails and an error message appears in the log file.

Problem

When you install or upgrade vRealize Automation, the procedure fails. This usually happens when a fix applied during install or upgrade is not successful. An error message appears in the log file similar to the following: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Cause

The Windows environment has a group policy for PowerShell script execution set to Enabled.

Solution

1. On the Windows host machine, run gedit.msc to open the Local Group Policy Editor.
2. In the left pane under Computer Configuration, click the expand button to open Administrative Templates > Windows Components > Windows PowerShell.
3. For Turn on Script Execution, change the state from Enabled to Not Configured.
Update Fails to Upgrade the Management Agent

An error message about the Management Agent appears when you click **Install Updates** on the vRealize Automation appliance management console Update Status page.

**Problem**

Upgrade process is unsuccessful. Message appears: Unable to upgrade management agent on node x. Sometimes the message lists more than one node.

**Cause**

Many conditions can cause this problem. The error message identifies only the node ID of the affected machine. More information is found in the All.log file for the Management Agent on the machine where the command fails.

Perform these tasks on the affected nodes according to your situation:

**Solution**

- If the Management Agent service is not running, start the service and restart upgrade on the virtual appliance.
- If the Management Agent service is running and the Management Agent is upgraded, restart upgrade on the virtual appliance.
- If the Management Agent service is running, but the Management Agent is not upgraded, perform a manual upgrade.
  
  a  Open a browser and navigate to the vRealize Automation IaaS installation page on the vRealize Automation appliance at **https://va-hostname.domain.name:5480/install**.
  b  Download and run the Management Agent Installer.
  c  Reboot the Management Agent machine.
  d  Restart upgrade on the virtual appliance.

Management Agent Upgrade is Unsuccessful

The Management Agent upgrade is unsuccessful while upgrading from vRealize Automation to 7.2 - 7.3.x.

**Problem**

If a failover incident has switched the primary and secondary Management Agent host, the upgrade is unsuccessful because the automated upgrade process cannot find the expected host. Perform this procedure on each IaaS node where the Management Agent is not upgraded.

**Solution**

1. Open the All.log in the Management Agent logs folder, which is located at **C:\Program Files (x86)\VMware\vCAC\Management Agent\Logs\**.

   The location of the installation folder might be different from the default location.
2 Search the log file for a message about an outdated or powered off virtual appliance.

For example, INNER EXCEPTION: System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond IP_Address:5480

3 Edit the Management Agent configuration file at C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config to replace the existing alternativeEndpointaddress value with the URL of the primary virtual appliance endpoint.

The location of the installation folder might be different from the default location.

Example of alternativeEndpointaddress in VMware.IaaS.Management.Agent.exe.config.

<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />

4 Restart the Management Agent Windows service and check the All.log file to verify that is working.

5 Run the upgrade procedure on the primary vRealize Automation appliance.

vRealize Automation Update Fails Because of Default Timeout Settings

You can increase the time setting for update if the default setting for synchronising databases is too short for your environment.

Problem

The timeout setting for the Vcac-Config SynchronizeDatabases command is not sufficient for some environments where synchronising databases takes longer than the default value of 3600 seconds.

The cafeTimeoutInSeconds and cafeRequestPageSize property values in the Vcac-Config.exe.config file govern the communication between the API and the Vcac-config.exe utility tool. The file is at IaaS installation location\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config.

You can override the default timeout value just for the SynchronizeDatabases command by supplying a value for these optional parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Short Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--DatabaseSyncTimeout</td>
<td>-dstm</td>
<td>Sets the http request timeout value only for SynchronizeDatabases in seconds.</td>
</tr>
<tr>
<td>--DatabaseSyncPageSize</td>
<td>-dsps</td>
<td>Sets the sync request page size only for Reservation or Reservation Policy synchronization. The default is 10.</td>
</tr>
</tbody>
</table>

If these parameters are not set in the Vcac-Config.exe.config file, the system uses the default timeout value.
Upgrading IaaS in a High Availability Environment Fails

Running the IaaS upgrade process on the primary web server node with load balancing enabled fails. You might see these error messages: "System.Net.WebException: The operation has timed out" or "401 - Unauthorized: Access is denied due to invalid credentials."

Problem

Upgrading IaaS with load balancing enabled can cause an intermittent failure. When this happens, you must run the vRealize Automation upgrade again with load balancing disabled.

Solution

1. Revert your environment to the pre-update snapshots.
2. Open a remote desktop connection to the primary IaaS web server node.
3. Navigate to the Windows hosts file at c:\windows\system32\drivers\etc.
4. Open the hosts file and add this line to bypass the web server load balancer.
   
   \text{IP\_address\_of\_primary\_iaas\_website\_node\ vrealizeautomation\_iaas\_website\_lb\_fqdn}
   
   Example:
   
   10.10.10.5 vra-iaas-web-lb.domain.com
5. Save the hosts file and retry the vRealize Automation update.
6. When the vRealize Automation update competes, open the hosts file and remove the line you added in step 4.

Work Around Upgrade Problems

You can modify the upgrade process to work around upgrade problems.

Solution

When you experience problems upgrading your vRealize Automation environment, use this procedure to modify the upgrade process by selecting one of the available flags.

Procedure

1. Open a secure shell connection to the primary vRealize Automation appliance node.
2 At the command prompt, run this command to create the toggle file:

\texttt{touch available\_flag}

For example: \texttt{touch /tmp/disable-iaas-upgrade}

\textbf{Table 1-89. Available Flags}

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
</table>
| /tmp/disable-iaas-upgrade | ■ Prevents IaaS upgrade process after the virtual appliance restarts.  
  ■ Prevents the Management Agent upgrade.  
  ■ Prevents the automatic prerequisite checks and fixes.  
  ■ Prevents stopping IaaS services. |
| /tmp/do-not-upgrade-ma | Prevents the Management Agent upgrade. This flag is suitable when the Management Agent is upgraded manually. |
| /tmp/skip-prereq-checks | Prevents the automatic prerequisite checks and fixes. This flag is suitable when there is a problem with the automatic prerequisite fixes and the fixes have been applied manually instead. |
| /tmp/do-not-stop-services | Prevents stopping IaaS services. The upgrade does not stop the IaaS Windows services, such as the Manager Service, DEMs, and agents. |
| /tmp/do-not-upgrade-servers | Prevents the automatic upgrade of all server IaaS components, such as the database, web site, WAPI, repository, Model Mfrorntanager data, and Manager Service. |
| /tmp/do-not-upgrade-dems | Prevents DEM upgrade. |
| /tmp/do-not-upgrade-agents | Prevents IaaS proxy agent upgrade. |

\textbf{Note} This flag also prevents enabling the Manager Service automatic failover mode.
3 Complete the tasks for your chosen flag.

### Table 1-90. Additional Tasks

<table>
<thead>
<tr>
<th>Flag</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/disable-iaas-upgrade</td>
<td></td>
</tr>
<tr>
<td></td>
<td>‣ Upgrade the Management Agent manually.</td>
</tr>
<tr>
<td></td>
<td>‣ Apply any required IaaS prerequisites manually.</td>
</tr>
<tr>
<td></td>
<td>‣ Manually stop the IaaS services.</td>
</tr>
<tr>
<td></td>
<td>a Log in to your IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>b Select Start &gt; Administrative Tools &gt; Services.</td>
</tr>
<tr>
<td></td>
<td>c Stop these services in the following order.</td>
</tr>
<tr>
<td></td>
<td>Note: Do not shut down the IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>a Each VMware vRealize Automation Proxy Agent.</td>
</tr>
<tr>
<td></td>
<td>b Each VMware DEM worker.</td>
</tr>
<tr>
<td></td>
<td>c The VMware DEM orchestrator.</td>
</tr>
<tr>
<td></td>
<td>d The VMware vCloud Automation Center service.</td>
</tr>
<tr>
<td></td>
<td>‣ Start the IaaS upgrade manually after the virtual appliance upgrade is complete.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-ma</td>
<td>Upgrade the Management Agent manually.</td>
</tr>
<tr>
<td>/tmp/skip-prereq-checks</td>
<td>Apply any required IaaS prerequisites manually.</td>
</tr>
<tr>
<td>/tmp/do-not-stop-services</td>
<td>Manually stop the IaaS services.</td>
</tr>
<tr>
<td></td>
<td>1 Log in to your IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>2 Select Start &gt; Administrative Tools &gt; Services.</td>
</tr>
<tr>
<td></td>
<td>3 Stop these services in the following order.</td>
</tr>
<tr>
<td></td>
<td>Note: Do not shut down the IaaS Windows server.</td>
</tr>
<tr>
<td></td>
<td>a Each VMware vRealize Automation Proxy Agent.</td>
</tr>
<tr>
<td></td>
<td>b Each VMware DEM worker.</td>
</tr>
<tr>
<td></td>
<td>c The VMware DEM orchestrator.</td>
</tr>
<tr>
<td></td>
<td>d The VMware vCloud Automation Center service.</td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-servers</td>
<td></td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-dems</td>
<td></td>
</tr>
<tr>
<td>/tmp/do-not-upgrade-agents</td>
<td></td>
</tr>
</tbody>
</table>

4 Access the primary vRealize Automation appliance management console and update the primary vRealize Automation appliance.

**Note** Because each flag remains active until it is removed, run this command to remove your chosen flag after upgrade: `rm /flag_path/flag_name`. For example, `rm /tmp/disable-iaas-upgrade`. 
**Virtual Appliance Upgrade Fails During the IaaS Prerequisite Check**

IaaS prerequisite check is unable to validate environments configured with a custom IIS website name. Disabling the automated IaaS upgrade corrects the problem.

**Problem**

The virtual appliance upgrade fails during the IaaS prerequisite check while running pre-install scripts and post-install scripts.

Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

When the failure occurs, you see an error message similar to: Applying automatic fix for `<prerequisite check name>` prerequisite failed.

**Cause**

IaaS prerequisite check is unable to validate environments configured with a custom IIS website name. Disabling the automated IaaS upgrade prerequisite checks corrects the problem.

**Solution**

1. Disable the automated IaaS upgrade prerequisite checks and fixes.
2. Run the vRealize Automation upgrade. See Work Around Upgrade Problems.
3. Follow the upgrade prompts. When the prompts direct you to reboot vRealize Automation, you can use the IaaS installer to search for any unsatisfied IaaS prerequisites and fix them manually.

**Note** Do not restart the appliance until you finish the IaaS prerequisites validation.

4. Use the following steps for every IaaS website node.
   a. Download the IaaS installer. See Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance.
   b. The first time you initialize the IaaS installer, it generates a new configuration file under the same directory with extension .exe.config.
   c. Close the IaaS installer and add the following key in the `<appSettings>` section of the configuration file. The key passes your custom website name to the IaaS prerequisite checker.

   `<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>`

   d. Save the configuration file and rerun the IaaS Installer. Follow the onscreen instructions, until the prerequisite validation is finished. If there were any failed prerequisites, fix them manually.
5 Activate the IaaS automatic upgrade by closing the IaaS installer and rebooting the upgraded vRealize Automation appliance.

**Note** If you decide to continue the IaaS upgrade manually using the IaaS Installer, first reboot the upgraded vRealize Automation appliance, wait for all services to become registered. You must upgrade and configure all systems that have IaaS components installed. For more information, see Upgrade the IaaS Components After Upgrading vRealize Automation 7.1 or 7.2 to 7.3.

---

**Migrating to vRealize Automation 7.4**

You can perform a side-by-side upgrade of your current vRealize Automation environment to the latest version using migration.

This information is specific to upgrading vRealize Automation to 7.4 using migration. For information about other supported upgrade paths, see Upgrading vRealize Automation.

**Migrating vRealize Automation**

You can perform a side-by-side upgrade of your current vRealize Automation environment using migration.

Migration moves all data, except for tenants and identity stores, from your current vRealize Automation source environment to a target deployment of the latest version of vRealize Automation. In addition, migration moves all data from the embedded vRealize Orchestrator 7.x to the target deployment.

Migration does not change your source environment except to stop vRealize Automation services for the time required to collect and copy the data safely to your target environment. Depending on the size of the source vRealize Automation database, migration can take from a few minutes to hours.

You can migrate your source environment to a minimal deployment or a high-availability deployment.

If you plan to put your target environment into production after migration, do not put your source environment back into service. Changes to your source environment after migration are not synchronized with your target environment.

If your source environment is integrated with vCloud Air or vCloud Director or has physical endpoints, you must use migration to perform an upgrade. Migration removes these endpoints and everything associated with them from the target environment. Migration also removes a 6.x VMware vRealize Application Services integration from the target environment.

**Note** You must complete additional tasks to prepare your vRealize Automation virtual machines before you migrate. Before you migrate, review Knowledge Base article 51531.

If you migrate from vRealize Automation 6.2.x to the latest version, you might experience these issues.
After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request.

- **Control types**: Check box or link.
- **Attributes**: Relationship, regular expressions, or property layouts.

In vRealize Automation 7.x, the property definitions no longer use these elements.

Regular expressions used to define the parent-child relationships in a vRealize Automation 6.2.x drop-down menu are not supported in 7.x. In 6.2.x, you can use regular expressions to define one or more child menu items that are only available for a certain parent menu item. Only those child menu items appear when you select the parent menu item.

After migration to 7.x, all the available menu items appear in the child drop-down menu regardless of what you choose in the parent drop-down menu. To show that previously defined dynamic values no longer work, the first menu item in the child drop-down menu reads “Warning! Use vRO workflows to define dynamic values.”

**Resolution**

You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see [Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request](#).

After migration, you must recreate the property definition to restore the previous dynamic values. For information about creating a parent-child relationship between the parent drop-down menu and the child drop-down menu, see [How to use dynamic property definitions in vRA 7.2](#).

---

**vRealize Automation Environment User Interfaces**

You use and manage your vRealize Automation environment with several interfaces.

**User Interfaces**

These tables describe the interfaces that you use to manage your vRealize Automation environment.

### Table 1-91. vRealize Automation Administration Console

<table>
<thead>
<tr>
<th><strong>Purpose</strong></th>
<th><strong>Access</strong></th>
<th><strong>Required Credentials</strong></th>
</tr>
</thead>
</table>
| You use the vRealize Automation console for these system administrator tasks. | 1. Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.  
2. Click **vRealize Automation console**.  
3. Log in. | You must be a user with the system administrator role. |
| - Add tenants.  
- Customize the vRealize Automation user interface.  
- Configure email servers.  
- View event logs.  
- Configure vRealize Orchestrator. |  

---

[Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request](#).

[How to use dynamic property definitions in vRA 7.2](#).
Table 1-92. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use vRealize Automation for these tasks.</td>
<td>1 Start a browser and enter the URL of your tenancy using the fully qualified domain name of the virtual appliance and the tenant URL name: <a href="https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name">https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name</a>.</td>
<td>You must be a user with one or more of these roles: Application Architect Approval Administrator Catalog Administrator Container Administrator Container Architect Health Consumer Infrastructure Architect Secure Export Consumer Software Architect Tenant Administrator XaaS Architect</td>
</tr>
<tr>
<td>Request new IT service blueprints.</td>
<td>2 Log in.</td>
<td></td>
</tr>
<tr>
<td>Create and manage cloud and IT resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and manage custom groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and manage business groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign roles to users.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 1-93. vRealize Automation Appliance Management. This interface is sometimes called the Virtual Appliance Management Interface (VAMI).

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use vRealize Automation Appliance Management for these tasks. | 1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name. | ▪ User name: root  
▪ Password: Password you entered when you deployed the vRealize Automation appliance. |
| ▪ View the status of registered services. | 2 Click vRealize Automation Appliance Management. You can also use this URL to open vRealize Automation Appliance Management: https://vra-va-hostname.domain.name:5480. |  |
| ▪ View system information and reboot or shutdown the appliance. | 3 Log in. |  |
| ▪ Manage participation in the Customer Experience Improvement Program. |  |  |
| ▪ View network status. |  |  |
| ▪ View update status and install updates. |  |  |
| ▪ Manage administration settings. |  |  |
| ▪ Manage vRealize Automation host settings. |  |  |
| ▪ Manage SSO settings. |  |  |
| ▪ Manage product licenses. |  |  |
| ▪ Configure the vRealize Automation Postgres database. |  |  |
| ▪ Configure vRealize Automation messaging. |  |  |
| ▪ Configure vRealize Automation logging. |  |  |
| ▪ Install IaaS components. |  |  |
| ▪ Migrate from an existing vRealize Automation installation. |  |  |
| ▪ Manage IaaS component certificates. |  |  |
| ▪ Configure Xenon service. |  |  |

Table 1-94. vRealize Orchestrator Client

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>You use the vRealize Orchestrator Client for these tasks.</td>
<td>1 Start a browser and open the vRealize Automation splash page using the fully qualified domain name of the virtual appliance: <a href="https://vra-va-hostname.domain.name">https://vra-va-hostname.domain.name</a>.</td>
<td>You must be a user with the system administrator role or part of the vcoadmins group configured in the vRealize Orchestrator Control Center Authentication Provider settings.</td>
</tr>
<tr>
<td>▪ Develop actions.</td>
<td>2 To download the client.jnlp file to your local computer, click vRealize Orchestrator Client.</td>
<td></td>
</tr>
<tr>
<td>▪ Develop workflows.</td>
<td>3 Right-click the client.jnlp file and select Launch.</td>
<td></td>
</tr>
<tr>
<td>▪ Manage policies.</td>
<td>4 On the Do you want to Continue? dialog box, click Continue.</td>
<td></td>
</tr>
<tr>
<td>▪ Install packages.</td>
<td>5 Log in.</td>
<td></td>
</tr>
<tr>
<td>▪ Manage user and user group permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Attach tags to URI objects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ View inventory.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-95. vRealize Orchestrator Control Center

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the vRealize Orchestrator Control Center to edit the configuration of the default vRealize Orchestrator instance that is embedded in vRealize Automation. | 1. Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.  
2. Click vRealize Automation Appliance Management.  
You can also use this URL to open vRealize Automation Appliance Management: https://vra-va-hostname.domain.name:5480.  
3. Log in.  
4. Click vRA Settings > Orchestrator.  
5. Select Orchestrator user interface.  
6. Click Start.  
7. Click the Orchestrator user interface URL.  
8. Log in. | User Name  
- Enter root if role-based authentication is not configured.  
- Enter your vRealize Automation user name if it is configured for role-based authentication.  
Password  
- Enter the password you entered when you deployed the vRealize Automation appliance if role-based authentication is not configured.  
- Enter the password for your user name if your user name is configured for role-based authentication. |

---

### Table 1-96. Linux Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You use the Linux command prompt on a host, such as the vRealize Automation appliance host, for these tasks.  
- Stop or start services  
- Edit configuration files  
- Run commands  
- Retrieve data | 1. On the vRealize Automation appliance host, open a command prompt.  
One way to open the command prompt on your local computer is to start a session on the host using an application such as PuTTY.  
2. Log in. | User name: root  
Password: Password you created when you deployed the vRealize Automation appliance. |

---

### Table 1-97. Windows Command Prompt

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Access</th>
<th>Required Credentials</th>
</tr>
</thead>
</table>
| You can use a Windows command prompt on a host, such as the IaaS host, to run scripts. | 1. On the IaaS host, log in to Windows.  
One way to log in from your local computer is to start a remote desktop session.  
2. Open the Windows command prompt.  
One way to open the command prompt is to right-click the Start icon on the host and select Command Prompt or Command Prompt (Admin). | User name: User with administrative privileges.  
Password: User’s password. |
Migration Prerequisites

The migration prerequisites differ depending on your target environment.

You can migrate to a minimal environment or to a high-availability environment.

Prerequisites for Migration to a Minimal Environment

Ensure a successful migration to a minimal environment by reviewing these prerequisites.

Minimal deployments include one vRealize Automation appliance and one Windows server that hosts the IaaS components. In a minimal deployment, the vRealize Automation SQL Server database can be on the same IaaS Windows server with the IaaS components, or on a separate Windows server.
Figure 1-19. vRealize Automation Minimal Deployment

- vRealize Automation Appliance
  - vRealize Orchestrator
  - PostgreSQL DB

- vRealize Automation Infrastructure as a service (IaaS)
  - Microsoft IIS
    - IaaS Web
    - Model Manager Repository
  - Manager Service
  - DEM Orchestrator
  - DEM Worker
  - Proxy Agent
  - Microsoft SQL Server DB
Prerequisites

- Verify that you have a new target environment of vRealize Automation.
- Install relevant proxy agents on the target environment according to these requirements.
  - Target proxy agent name must match the source proxy agent name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.

  **Note** Finish these steps to obtain an agent name.
  1. On the IaaS host, log in to Windows as a local user with **administrator** privileges.
  2. Use Windows Explorer to go to the agent installation directory.
  3. Open the `VRMAgent.exe.config` file.
  4. Under the `serviceConfiguration` tag, look for the value of the `agentName` attribute.

- Review Knowledge Base article [51531](#).
- Target proxy agent endpoint name must match the source proxy agent endpoint name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.
- Do not create an endpoint for vSphere, Hyper-V, Citrix XenServer, or Test proxy agents on the target environment.

- Review the version numbers of vRealize Automation components on the target vRealize Automation appliance.
  a. Log in to the target vRealize Automation Appliance Management as **root** using the password you entered when you deployed the target vRealize Automation appliance.
  b. Select **vRA Settings > Cluster**.
  c. Expand the Host / Node Name records by clicking the triangle.

  Verify that the version numbers of the vRealize Automation IaaS components match.

- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.

- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.

- Verify that the endpoint vCenter has sufficient resources to complete migration.

- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.

- Verify that the IaaS server node in the target environment has at least Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. After you install the JRE, make sure the JAVA_HOME environment variable points to the Java version you installed on each IaaS node. Revise the path if necessary.

- Verify that each IaaS node has PowerShell 3.0 or later installed.
- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.
- Verify that the IaaS Web Service and Model Manager do not need to be restarted because of pending Windows installation updates. Pending updates might prevent the migration to begin or end the World Wide Web Publishing Service.

**What to do next**

**Pre-Migration Tasks.**

**Prerequisites for Migration to a High-Availability Environment**

Ensure a successful migration to a high-availability environment by reviewing these prerequisites.

High-availability environments can be of varying size. A basic distributed deployment might improve vRealize Automation simply by hosting IaaS components on separate Windows servers. Many high-availability environments go even further, with redundant appliances, redundant servers, and load balancing for even more capacity. Large, distributed deployments provide for better scale, high availability, and disaster recovery.
Figure 1-20. vRealize Automation High-Availability Environment
Prerequisites

- Verify that you have a new target installation of vRealize Automation with a master and replica virtual appliance configured for high availability. See vRealize Automation High Availability Configuration Considerations.
- Verify that all vRealize Automation virtual appliances use the same password for root user.
- Install relevant proxy agents on the target environment according to these requirements.
  - Target proxy agent name must match the source proxy agent name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.

**Note** Finish these steps to obtain an agent name.

1. On the IaaS host, log in to Windows as a local user with administrator privileges.
2. Use Windows Explorer to go to the agent installation directory.
3. Open the VRMAgent.exe.config file.
4. Under the serviceConfiguration tag, look for the value of the agentName attribute.

- Target proxy agent endpoint name must match the source proxy agent endpoint name for vSphere, Hyper-V, Citrix XenServer, and Test proxy agents.
- Do not create an endpoint for vSphere, Hyper-V, Citrix XenServer, or Test proxy agents on the target environment.
- Check the version numbers of vRealize Automation components on the target vRealize Automation appliance.
  b. Log in with the user name root and the password you entered when you deployed the appliance.
  c. Select vRA Settings > Cluster.
  d. To expand the Host / Node Name records so you can see the components, click the expand button.
     - Verify that the version numbers of vRealize Automation components match across all virtual appliance nodes.
     - Verify that the version numbers of vRealize Automation IaaS components match across all IaaS nodes.
- Review Knowledge Base article 51531.
- Perform these steps to direct traffic to only the master node.
  a. Disable all the redundant nodes.
b  Remove the health monitors for these items according to your load balancer documentation:
   - vRealize Automation virtual appliance
   - IaaS Website
   - IaaS Manager Service

- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.
- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.
- Verify that the endpoint vCenter has sufficient resources to complete migration.
- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.
- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.
- Verify that the IaaS Web Service and Model Manager nodes in the target environment have the right Java Runtime Environment. You must have Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. Make sure the JAVA_HOME system variable points to the Java version you installed on each IaaS node. Revise the path if necessary.
- Verify that each IaaS node has at least PowerShell 3.0 or later installed.
- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.
- Verify that the IaaS Web Service and Model Manager do not need to be restarted because of pending Windows installation updates. Pending updates might prevent the migration to begin or end the World Wide Web Publishing Service.

What to do next

Pre-Migration Tasks.

Pre-Migration Tasks

Before you migrate, you must perform several pre-migration tasks.

The pre-migration tasks you perform before you migrate your source vRealize Automation environment data to the target vRealize Automation environment vary depending on your source environment.
Review Changes Introduced by Migration from vRealize Automation 6.2.x to 7.x

vRealize Automation 7 and later introduces various functional changes during and after the upgrade process. Review these changes before you upgrade your vRealize Automation 6.2.x deployment to the latest version.

For information about the differences between vRealize Automation 6.2.x and 7.x, see Considerations About Upgrading to This vRealize Automation Version in Upgrading vRealize Automation 6.2.5 to 7.4.

Note: The vRealize Production Test Upgrade Assist Tool analyzes your vRealize Automation 6.2.x environment for any feature configuration that can cause upgrade issues and checks that your environment is ready for upgrade. To download this tool and related documentation, go to the VMware vRealize Production Test Tool download product page.

After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request.

- Control types: Check box or link.
- Attributes: Relationship, regular expressions, or property layouts.

In vRealize Automation 7.x, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request.

Apply Software Agent Patch

Before you migrate from vRealize Automation 7.1 or 7.3 to 7.4, you must apply a hot fix to the source appliance so that you can upgrade Software Agents to TLS 1.2.

The Transport Layer Security (TLS) protocol provides data integrity between your browser and vRealize Automation. This hot fix makes it possible for the Software Agents in your source environment to upgrade to TLS 1.2. This upgrade ensures the highest level of security and is required for vRealize Automation 7.1 or 7.3. Each version has its own hot fix.

Prerequisites

A running vRealize Automation 7.1 or 7.3 source environment.

Procedure

- Apply this hot fix to your source vRealize Automation 7.1 or 7.3 appliance before you migrate to 7.4. See Knowledge Base article 52897.

What to do next

Change DoDeletes Setting on the vSphere Agent to False.

Change DoDeletes Setting on the vSphere Agent to False

If you migrate from a vRealize Automation 6.2.x environment, you must change the DoDeletes value from true to false on your target vSphere agent before migration.
Prerequisites

Finish the prerequisites for migration.

Procedure

1. Change the DoDeletes value to false. This prevents deletion of your virtual machines from the source environment. The source and target environments run in parallel. Lease discrepancies might arise after the production migration is validated.

2. Set the DoDeletes value to true after your production migration is validated and your source environment shuts down.

3. Follow the steps in the Configure the vSphere Agent procedure to set DoDeletes to false.

What to do next

Prepare vRealize Automation Virtual Machines for Migration.

Check Templates in Your vRealize Automation Source Environment

Before you migrate vRealize Automation, you must check your virtual machine templates to make sure that every template has a minimum memory setting of at least 4 MB.

If you have a virtual machine template in your vRealize Automation source environment with less than 4 MB of memory, migration fails. Complete this procedure to determine if any blueprints in the source environment have less than 4 MB of memory.

Prerequisites

Procedure

1. Log in to the windows server hosting your SQL server database.

2. Open the SQL Server Management Studio and connect to your vRA database.

3. Run this script to check if there are any blueprints with memory specified at less than 4 MB.

   ```sql
   select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and MemoryMB < 4;
   ```

   where vCAC is the database name.

4. If the script finds any blueprints with memory specified at less than 4 MB, then run this script to update the memory to at least 4 MB.

   ```sql
   update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
   ```

   where vCAC is the database name.

What to do next

Prepare vRealize Automation Virtual Machines for Migration.
Prepare vRealize Automation Virtual Machines for Migration

Known issues with migrating vRealize Automation 6.2.x virtual machines can cause problems after migration.

You must review Knowledge Base article 000051531 and perform any relevant fixes to your environments prior to migration.

What to do next

Gather Information Required for Migration.

Gather Information Required for Migration

Use these tables to record the information that you need for migration from your source and target environments.

Prerequisites

Finish verifying the prerequisites for your situation.

- Prerequisites for Migration to a Minimal Environment.
- Prerequisites for Migration to a High-Availability Environment.

Table 1-98. Source vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Log in to your source vRealize Automation Appliance Management. Find the host name on the System tab. The host name must be a fully qualified domain name (FQDN).</td>
<td></td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed your source vRealize Automation appliance.</td>
<td></td>
</tr>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created. The directory must have available space that is twice as big as the size of the vRealize Automation database. The default location is /storage.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-99. Target vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed your target vRealize Automation appliance.</td>
<td></td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local</td>
<td></td>
</tr>
</tbody>
</table>
Table 1-99. Target vRealize Automation Appliance (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator username</td>
<td></td>
<td>administrator</td>
</tr>
<tr>
<td>Administrator password</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-100. Target IaaS Database

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>Location of Microsoft SQL Server instance where the cloned database resides. If named instance and a non-default port is used, specify in SERVER,PORT\INSTANCE-NAME format.</td>
<td></td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation6.2.x/7.x IaaS Microsoft SQL database cloned for migration.</td>
<td></td>
</tr>
<tr>
<td>Authentication mode</td>
<td>Select either Windows or SQL Server. If you select SQL Server, you must enter a login name and password.</td>
<td></td>
</tr>
<tr>
<td>Login name</td>
<td>Login name for the SQL Server user who has the db_owner role for the cloned IaaS Microsoft SQL database.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SQL Server user.</td>
<td></td>
</tr>
<tr>
<td>Original encryption key</td>
<td>Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment.</td>
<td></td>
</tr>
<tr>
<td>New passphrase</td>
<td>A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment.</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

**Obtain the Encryption Key from the Source vRealize Automation Environment.**

**Obtain the Encryption Key from the Source vRealize Automation Environment**

You must enter the encryption key from the source vRealize Automation environment as part of the migration procedure.

**Prerequisites**

Verify that you have administrator privileges on the active Manager Service host virtual machine in your source environment.
Procedure

1. Open a command prompt as an administrator on the virtual machine that hosts the active Manager Service in your source environment and run this command.

   "C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config" -v

   If your installation directory is not in the default location, C:\Program Files (x86)\VMware\vCAC, edit the path to show your actual installation directory.

2. Save the key that appears after you run the command.

   The key is a long string of characters that looks similar to this example:

   NRH+f/BlnCB6yvasLS3sxespdkcFWAEuyV0g4lfryg=

What to do next

- If you are migrating from a vRealize Automation 6.2.x environment: Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.

- If you are migrating from a vRealize Automation 7.x environment: List Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment.

List Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment

Before you migrate a vRealize Automation 6.2.x environment, you must make a list of the tenant and IaaS administrators for each tenant.

Perform the following procedure for each tenant in the source vRealize Automation console.

**Note** If you migrate from a vRealize Automation 7.x environment, you do not need to perform this procedure.

Prerequisites

Log in to the source vRealize Automation console as Administrator with the password you entered when you deployed the source vRealize Automation appliance.

**Note** For a high-availability environment, open the console using the fully qualified domain name of the source virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

Procedure

1. Select Administration > Tenants.

2. Click a tenant name.

3. Click Administrators.

4. Make a list of each tenant and IaaS administrator user name.
5  Click Cancel.

What to do next

Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.

Add Each Tenant from the Source vRealize Automation Environment to the Target Environment

You must add tenants in the target environment using the name of each tenant in the source environment. For successful migration, it is mandatory that each tenant in the source environment is created in the target environment. You must also use a tenant-specific access URL for each tenant that you add using the tenant URL name from the source environment. If there are unused tenants in the source environment that you do not want to migrate, delete them from the source environment before migration.

Note  Migration validation ensures that the target system has at least the same tenants configured in the source as required by the prerequisites. It performs tenant comparison based on case-sensitive tenant URL names, not the tenant names.

Perform this procedure for each tenant in your source environment.

- When you migrate from a vRealize Automation 6.2.x environment, you migrate your existing SSO2 tenants and identity stores on the source environment to the VMware Identity Manager on the target environment.
- When you migrate from a vRealize Automation 7.x environment, you migrate your existing VMware Identity Manager tenants and identity stores on the source environment to the VMware Identity Manager on the target environment.

Prerequisites

- Gather Information Required for Migration.
- Log in to the target vRealize Automation console as Administrator with the password you entered when you deployed the target vRealize Automation appliance.

Note  For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

Procedure

1  Select Administration > Tenants.

2  Click the New icon (➕).

3  In the Name text box, enter a tenant name that matches a tenant name in the source environment. For example, if the tenant name in the source environment is DEVTenant, enter DEVTenant.

4  (Optional) Enter a description in the Description text box.
5 In the **URL Name** text box, enter a tenant URL name that matches the tenant URL name in the source environment.

The URL name is used to append a tenant-specific identifier to the vRealize Automation console URL.

For example, if the URL name for DEVTenant in the source environment is dev, enter `dev` to create the URL `https://vra-va-hostname.domain.name/vcac/org/dev`.

6 (Optional) Enter an email address in the **Contact Email** text box.

7 Click **Submit and Next**.

**What to do next**

Create an Administrator for Each Added Tenant.

**Create an Administrator for Each Added Tenant**

You must create an administrator for each tenant that you added to the target environment. You create an administrator by creating a local user account and assigning tenant administrator privileges to the local user account.

Perform this procedure for each tenant in your target environment.

**Prerequisites**

- **Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.**
- Log in to the target vRealize Automation console as **Administrator** with the password you entered when you deployed the target vRealize Automation appliance.

**Note** For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: `https://vra-va-lb-hostname.domain.name/vcac`.

**Procedure**

1 Select **Administration > Tenants**.

2 Click a tenant that you added.

   For example, for DEVTenant, click **DEVTenant**.

3 Click **Local users**.

4 Click the **New** icon (`➕`).

5 In **User Details**, enter the requested information to create a local user account to assign the tenant administrator role.

   The local user name must be unique to the default local directory, vsphere.local.

6 Click **OK**.

7 Click **Administrators**.
8 Enter the local user name in the **Tenant administrators** search box and press Enter.

9 Click the appropriate name in the search returns to add the user to the list of tenant administrators.

10 Click **Finish**.

11 Log out of the console.

**What to do next**

- For a minimal deployment: Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment.
- For a high-availability deployment: Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment.

**Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment**

Before you import your users and groups to a minimal deployment of vRealize Automation, you must connect the target vRealize Automation to your Active Directory link.

Perform this procedure for each tenant. If a tenant has more than one Active Directory, perform this procedure for each Active Directory that the tenant uses.

**Prerequisites**

- Create an Administrator for Each Added Tenant.
- Verify that you have access privileges to the Active Directory.
- Log in to vRealize Automation as a **tenant administrator**.

**Procedure**

1 Select **Administration > Directories Management > Directories**.

2 Click **Add Directory** icon ( ) and select **Add Active Directory over LDAP/IWA**.

3 Enter your Active Directory account settings.

   - **For Non-Native Active Directories**

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>Enter a unique directory name. Select <strong>Active Directory over LDAP</strong> when using Non-Native Active Directory.</td>
</tr>
<tr>
<td>This Directory Supports DNS Service Location</td>
<td>Deselect this option.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the distinguished name (DN) of the starting point for directory server searches. For example, <code>cn=users,dc=rainpole,dc=local</code>.</td>
</tr>
</tbody>
</table>
### Bind DN
Enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.
For example, `cn=config_admin infra,cn=users,dc=rainpole,dc=local`.

### Bind DN Password
Enter the Active Directory password for the account that can search for users and click **Test Connection** to test the connection to the configured directory.

**For Native Active Directories**

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory Name</strong></td>
<td>Enter a unique directory name. Select <a href="integrated-into-windows-authentication">Active Directory (Integrated Windows Authentication)</a> when using Native Active Directory.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Enter the name of the domain to join.</td>
</tr>
<tr>
<td><strong>Domain Admin Username</strong></td>
<td>Enter the user name for the domain admin.</td>
</tr>
<tr>
<td><strong>Domain Admin Password</strong></td>
<td>Enter the password for the domain admin.</td>
</tr>
<tr>
<td><strong>Bind User UPN</strong></td>
<td>Use the email address format to enter the name of the user who can authenticate with the domain.</td>
</tr>
<tr>
<td><strong>Bind DN Password</strong></td>
<td>Enter the Active Directory bind account password for the account that can search for users.</td>
</tr>
</tbody>
</table>

1. Click **Save & Next**.
2. **Select the Domains** displays a list of domains.
3. Accept the default domain setting and click **Next**.
4. Verify that the attribute names are mapped to the correct Active Directory attributes, and click **Next**.
5. Select the groups and users to synchronize.
   a. Click the **New** icon (➕).
   b. Enter the user domain and click **Find Groups**.
      For example, enter `dc=vcac,dc=local`.
   c. To select the groups to synchronize, click **Select** and click **Next**.
   d. On **Select Users**, select the users to synchronize and click **Next**.
      Only add users and groups that are required to use vRealize Automation. Do not select **Sync nested groups** unless all of the groups in the nest are required to use vRealize Automation.
6. Review the users and groups you are syncing to the directory, and click **Sync Directory**.
   The directory synchronization takes some time and runs in the background.

**What to do next**

Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment
Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment

Before you import your users and groups to a high-availability vRealize Automation environment, you must connect to your Active Directory link.

- Perform steps 1-8 for each tenant. If a tenant has more than one Active Directory, perform this procedure for each Active Directory that the tenant uses.
- Repeat steps 9–10 for each identity provider associated with a tenant.

Prerequisites

- Create an Administrator for Each Added Tenant.
- Verify that you have access privileges to the Active Directory.
- Log in to vRealize Automation as a tenant administrator.

Procedure

1. Select **Administration > Directories Management > Directories**.
2. Click **Add Directory** icon (⊕) and select **Add Active Directory over LDAP/IWA**.
3. Enter your Active Directory account settings.
   - For Non-Native Active Directories
     - **Directory Name**: Enter a unique directory name.
     - **Select Active Directory over LDAP** when using Non-Native Active Directory.
     - **This Directory Supports DNS Service Location**: Deselect this option.
     - **Base DN**: Enter the distinguished name (DN) of the starting point for directory server searches.
       For example, `cn=users,dc=rainpole,dc=local`.
     - **Bind DN**: Enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.
       For example, `cn=config_admin_infra,cn=users,dc=rainpole,dc=local`.
     - **Bind DN Password**: Enter the Active Directory password for the account that can search for users and click **Test Connection** to test the connection to the configured directory.
   - For Native Active Directories
     - **Directory Name**: Enter a unique directory name.
     - **Select Active Directory (Integrated Windows Authentication)** when using Native Active Directory.
     - **Domain Name**: Enter the name of the domain to join.
     - **Domain Admin Username**: Enter the user name for the domain admin.
     - **Domain Admin Password**: Enter the password for the domain admin account.
<table>
<thead>
<tr>
<th>Option</th>
<th>Sample Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind User UPN</td>
<td>Use the email address format to enter the name of the user who can authenticate with the domain.</td>
</tr>
<tr>
<td>Bind DN Password</td>
<td>Enter the Active Directory bind account password for the account that can search for users.</td>
</tr>
</tbody>
</table>

4. Click **Save & Next**.

   The **Select the Domains** page displays the list of domains.

5. Accept the default domain setting and click **Next**.

6. Verify that the attribute names are mapped to the correct Active Directory attributes, and click **Next**.

7. Select the groups and users to synchronize.
   
   a. Click the **New** icon.
   
   b. Enter the user domain and click **Find Groups**.
      
      For example, enter `dc=vcac,dc=local`.
   
   c. To select the groups to synchronize, click **Select** and click **Next**.
   
   d. On the **Select Users** page, select the users to synchronize and click **Next**.
      
      Only add users and groups that are required to use vRealize Automation. Do not select **Sync nested groups** unless all of the groups in the nest are required to use vRealize Automation.

8. Review the users and groups you are syncing to the directory, and click **Sync Directory**.

   The directory synchronization takes some time and runs in the background.


   For example, **WorkspaceIDP__1**.

10. On the page for the identity provider that you selected, add a connector for each node.

    a. Follow the instructions for **Add a Connector**.
    
    b. Update the value for the **IdP Hostname** property to point to the fully qualified domain name (FQDN) for the vRealize Automation load balancer.
    
    c. Click **Save**.

**What to do next**

**Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.**

**Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment**

Before you migrate, you must run NSX Network and Security Inventory data collection in the source vRealize Automation environment.
This data collection is necessary for the Load Balancer Reconfigure action to work in vRealize Automation 7.4 when you migrate from 7.1, 7.2, or 7.3 deployments.

**Note**  You do not need to run this data collection in your source environment when you migrate from vRealize Automation 6.2.x. vRealize Automation 6.2.x does not support the Load Balancer Reconfigure action.

**Procedure**

- Run NSX Network and Security Inventory data collection in your source vRealize Automation environment before you migrate to vRealize Automation 7.4. See Start Endpoint Data Collection Manually in Managing vRealize Automation.

**What to do next**

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.

**Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database**

Before migration, you must back up your IaaS Microsoft SQL database in the vRealize Automation source environment and restore it to a new blank database created in the vRealize Automation target environment.

**Prerequisites**

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.
- Obtain information about backing up and restoring an SQL Server database. Find articles on the Microsoft Developer Network about creating a full SQL Server database backup and restoring an SQL Server database to a new location.

**Procedure**

- Create a full backup of your source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database. You use the backup to restore the SQL database to a new blank database created in the target environment.

**What to do next**

Snapshot the Target vRealize Automation Environment.

**Snapshot the Target vRealize Automation Environment**

Take a snapshot of each target vRealize Automation virtual machine. If migration is unsuccessful, you can try again using the virtual machine snapshots.

For information, see your vSphere documentation.

**Prerequisites**

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
What to do next

Perform one of the following procedures:

- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment.
- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

Migration Procedures

The procedure you perform to migrate your source vRealize Automation environment data depends on whether you migrate to a minimal environment or to a high-availability environment.

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4.

All tenants in the source system must be recreated in the target and go through the Migrate Identity Stores procedure. For more information, see Migrate Identity Stores to VMware Identity Manager.

Prerequisites

- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment.
- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as root using the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1. Select vRA Settings > Migration.

2. Enter the information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name for the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the vRealize Automation appliance.</td>
</tr>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created.</td>
</tr>
</tbody>
</table>
3 Enter the information for the target vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the target vRealize Automation appliance.</td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>Administrator username</td>
<td>administrator</td>
</tr>
<tr>
<td>Administrator password</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>

4 Enter the information for the target IaaS database server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>The location of the Microsoft SQL Server where the restored vRealize Automation IaaS Microsoft SQL database resides. If a named instance and a non-default port are used, enter in SERVER,PORT.INSTANCE-NAME format. If you configure the target Microsoft SQL Server to use the AlwaysOn Availability Group (AAG) feature, the target SQL Server should be entered as the AAG listener name, without a port or instance name.</td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.</td>
</tr>
</tbody>
</table>
| Authentication mode    | ■ Windows
  If you use the Windows authentication mode, the IaaS service user must have the SQL Server db_owner role. The same permissions apply when using SQL Server authentication mode.  
  ■ SQL Server
  SQL Server opens the Login name and Password text boxes. |
| Login name             | Login name of the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.                                          |
| Password               | Password for the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.                                           |
| Original encryption key| Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment. |
| New passphrase         | A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment. |

5 Click Validate.

The page displays the validation progress.

- If all the items validate successfully, go to step 8.
If an item fails to validate, inspect the error message and the validation log file on the IaaS nodes. For log file locations, see Migration Log Locations. Click Edit Settings and edit the problem item. Go to step 7.

6 Click Migrate.

The page displays the migration progress.
- If migration is successful, the page displays all migration tasks as completed.
- If migration is unsuccessful, inspect the migration log files on the virtual appliance and the IaaS nodes. For log file locations, see Migration Log Locations.

Finish these steps before you restart migration.
- a Revert your target vRealize Automation environment to the state you captured when you took a snapshot before migration.
- b Restore your target IaaS Microsoft SQL database using the backup of the source IaaS database.

What to do next

Post-Migration Tasks.

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4 configured as a high-availability environment.

All tenants in the source system must be recreated in the target and go through the Migrate Identity Stores procedure. For more information, see Migrate Identity Stores to VMware Identity Manager.

Prerequisites
- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment.
- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as root using the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1 Select vRA Settings > Migration.
2 Enter the information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name for the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the source vRealize Automation appliance.</td>
</tr>
</tbody>
</table>

3 Enter the information for the migration package location on the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration package location</td>
<td>Path to an existing directory on the source vRealize Automation 6.2.x or 7.x appliance where the migration package is created.</td>
</tr>
</tbody>
</table>

4 Enter the information for the target vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Root password</td>
<td>The root password that you entered when you deployed the target vRealize Automation appliance.</td>
</tr>
<tr>
<td>Default tenant</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>Administrator username</td>
<td>administrator</td>
</tr>
<tr>
<td>Administrator password</td>
<td>Password for the <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> user that you entered when you deployed the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>

5 Enter the information for the target IaaS database server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td>The location of the Microsoft SQL Server instance where the restored vRealize Automation IaaS Microsoft SQL database resides. If a named instance and a non-default port are used, enter in SERVER,PORT\INSTANCE-NAME format. If you configure the target Microsoft SQL Server to use the AlwaysOn Availability Group (AAG) feature, the target SQL Server should be entered as the AAG listener name, without a port or instance name.</td>
</tr>
<tr>
<td>Cloned database name</td>
<td>Name of the source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.</td>
</tr>
<tr>
<td>Authentication mode</td>
<td>- Windows&lt;br&gt;If you use the Windows authentication mode, the IaaS service user must have the SQL Server db_owner role. The same permissions apply when using SQL Server authentication mode.&lt;br&gt;- SQL Server&lt;br&gt;SQL Server opens the Login name and Password text boxes.</td>
</tr>
<tr>
<td>Login name</td>
<td>Login name of the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SQL Server user with the db_owner role for the cloned IaaS Microsoft SQL database.</td>
</tr>
<tr>
<td>Original encryption key</td>
<td>Original encryption key that you retrieve from the source environment. See Obtain the Encryption Key from the Source vRealize Automation Environment.</td>
</tr>
<tr>
<td>New passphrase</td>
<td>A series of words used to generate a new encryption key. You use this passphrase each time you install a new IaaS component in the target vRealize Automation environment.</td>
</tr>
</tbody>
</table>

6 Click **Validate**.

The page displays the validation progress.

- If all the items validate successfully, go to step 8.
- If an item fails to validate, inspect the error message and the validation log file on the IaaS nodes. For log file locations, see Migration Log Locations. Click **Edit Settings** and edit the problem item. Go to step 7.

7 Click **Migrate**.

The page displays the migration progress.

- If migration is successful, the page displays all migration tasks as completed.
- If migration is unsuccessful, inspect the migration log files on the virtual appliance and the IaaS nodes. For log file locations, see Migration Log Locations.

Finish these steps before you restart migration:

a Revert your target vRealize Automation environment to the state you captured when you took a snapshot before migration.

b Restore your target IaaS Microsoft SQL database using the backup of the source IaaS database.

**What to do next**

**Post-Migration Tasks.**

**Post-Migration Tasks**

After you migrate vRealize Automation, perform the post-migration tasks that pertain to your situation.

**Note** After you migrate the identity stores, users of vRealize Code Stream must manually reassign vRealize Code Stream roles.

**Add Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment**

You must delete and restore the vRealize Automation 6.2.x tenant administrators in each tenant after migration.

Perform the following procedure for each tenant in the target vRealize Automation console.

**Note** If you migrate from a vRealize Automation 7.x environment, you do not need to perform this procedure.
Prerequisites

- Successful migration to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console as Administrator with the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1. Select Administration > Tenants.
2. Click a tenant name.
3. Click Administrators.
4. Make a list of each tenant administrator name and user name.
5. Point to each administrator and click the delete icon (Delete) until you delete all administrators.
6. Click Finish.
7. On the Tenants page, click the tenant name again.
8. Click Administrators.
9. Enter the name of each user that you deleted in the appropriate search box and press Enter.
10. Click the name of the appropriate user from the search returns to add the user back as an administrator.

   When you finish, the list of tenant administrators looks the same as the list of administrators you deleted.
11. Click Finish.

Run Test Connection and Verify Migrated Endpoints

Migrating to vRealize Automation 7.4 makes changes to endpoints in the target environment.

After you migrate to vRealize Automation 7.4, you must use the Test Connection action for all applicable endpoints. You might also need to make adjustments to some migrated endpoints. For more information, see Considerations When Working With Upgraded or Migrated Endpoints.

The default security setting for upgraded or migrated endpoints is not to accept untrusted certificates.

After upgrading or migrating from an earlier vRealize Automation installation, if you were using untrusted certificates you must perform the following steps for all vSphere and NSX endpoints to enable certificate validation. Otherwise, the endpoint operations fail with certificate errors. For more information, see VMware Knowledge Base articles Endpoint communication is broken after upgrade to vRA 7.3 (2150230) at http://kb.vmware.com/kb/2150230 and How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294) at http://kb.vmware.com/kb/2108294.

1. After upgrade or migration, log in to the vRealize Automation vSphere agent machine and restart your vSphere agents by using the Services tab.

   Migration might not restart all agents, so manually restart them if needed.
2  Wait for at least one ping report to finish. It takes a minute or two for a ping report to finish.

3  When the vSphere agents have started data collection, log in to vRealize Automation as an IaaS administrator.

4  Click Infrastructure > Endpoints > Endpoints.

5  Edit a vSphere endpoint and click Test Connection.

6  If a certificate prompt appears, click OK to accept the certificate.
   
   If a certificate prompt does not appear, the certificate might currently be correctly stored in a trusted root authority of the Windows machine hosting service for the endpoint, for example as a proxy agent machine or DEM machine.

7  Click OK to apply the certificate acceptance and save the endpoint.

8  Repeat this procedure for each vSphere endpoint.

9  Repeat this procedure for each NSX endpoint.

If the Test Connection action is successful but some data collection or provisioning operations fail, you can install the same certificate on all the agent machines that serve the endpoint and on all DEM machines. Alternatively, you can uninstall the certificate from existing machines and repeat the preceding procedure for the failing endpoint.

Run NSX Network and Security Inventory Data Collection in Your Target vRealize Automation 7.4 Environment

After you migrate, you must run NSX Network and Security Inventory data collection in the target vRealize Automation 7.4 environment.

This data collection is necessary for the Load Balancer Reconfigure action to work in vRealize Automation 7.4 for 7.1, 7.2, and 7.3 deployments.

**Note** You do not need to perform this data collection if you migrated from vRealize Automation 6.2.x to 7.4.

**Prerequisites**

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.
- Successfully migrate to vRealize Automation 7.4.

**Procedure**

- Run NSX Network and Security Inventory data collection in your target vRealize Automation environment before you migrate to vRealize Automation 7.4. See Start Endpoint Data Collection Manually in Managing vRealize Automation.

**Reconfigure Load Balancers After Migration to a High-Availability Environment**

When you migrate to a high-availability environment, you must perform these tasks for each load balancer after you finish migration.
Prerequisites

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

Procedure

1. Restore the original health check settings so replica nodes can accept incoming traffic by configuring the load balancers for these items.
   - vRealize Automation appliance.
   - IaaS Web Server that hosts the Model Manager.
   - Manager Service.

2. Change the load balancer timeout settings back to the default.

Migrating an External Orchestrator Server to vRealize Automation 7.4

You can migrate your existing external Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation.

You can deploy vRealize Orchestrator as an external server instance and configure vRealize Automation to work with that external instance, or you can configure and use the vRealize Orchestrator server that is included in the vRealize Automation appliance.

VMware recommends that you migrate your external vRealize Orchestrator to the Orchestrator server that is built into vRealize Automation. The migration from an external to embedded Orchestrator provides the following benefits:

- Reduces the total cost of ownership.
- Simplifies the deployment model.
- Improves the operational efficiency.

Note: Consider using the external vRealize Orchestrator in the following cases:

- Multiple tenants in the vRealize Automation environment.
- Geographically dispersed environment.
- Workload handling.
- Use of specific plug-ins, such as the Site Recovery Manager plug-in versions earlier than 6.5.

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.
## Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

<table>
<thead>
<tr>
<th>vRealize Orchestrator Deployment</th>
<th>vRealize Automation Deployment</th>
<th>Migration Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Orchestrator 6.0.3 Virtual Appliance</td>
<td>vRealize Automation 6.2.3</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.4 on Windows</td>
<td>vRealize Automation 6.2.4</td>
<td>Migrate an External vRealize Orchestrator 6.x on Windows to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.4 Virtual Appliance</td>
<td>vRealize Automation 6.2.4</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.5 Virtual Appliance</td>
<td>vRealize Automation 6.2.5</td>
<td>Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12c</td>
<td>vRealize Automation 7.0 or IaaS</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database</td>
<td>vRealize Automation 7.0.1 or IaaS</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.1 Virtual Appliance</td>
<td>vRealize Automation 7.1</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.2 Virtual Appliance</td>
<td>vRealize Automation 7.2</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</td>
</tr>
<tr>
<td>vRealize Orchestrator 7.3 Virtual Appliance</td>
<td>vRealize Automation 7.3</td>
<td>Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4</td>
</tr>
<tr>
<td>vRealize Orchestrator 6.0.3 on Windows</td>
<td>vRealize Automation 6.2.3</td>
<td>Migrate the Orchestrator Configuration from Windows to Virtual Appliance</td>
</tr>
</tbody>
</table>

## Migrate the Orchestrator Configuration from Windows to Virtual Appliance

Migrate your 5.5.x and 6.x Orchestrator Windows standalone configuration to the Orchestrator Appliance.

### Prerequisites

- Deploy and configure an Orchestrator node on the target version. See Configuring a Standalone Orchestrator Server.
- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.
- Stop the Orchestrator server service on both the source and the target Orchestrator instances.
Back up the source Orchestrator database, including the database schema.

**Note** If you plan to preserve the source Orchestrator environment after migration, clone the source Orchestrator database to another database. Afterwards, configure the target Orchestrator to use the cloned instance, instead of the instance configured during installation. If you skip this step, the target Orchestrator will upgrade the source Orchestrator database and it will no longer work with the source Orchestrator environment.

**Procedure**

1. Download the migration tool from the target Orchestrator server.
   a. Log in to Control Center as **root**.
   b. Open the **Export/Import Configuration** page and click the **Import Configuration** tab.
   c. Download the migration tool as specified in the description on the page, or download it directly from https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool.

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. Extract the downloaded archive in the Orchestrator install folder.
      The default path to the Orchestrator install folder in a Windows-based installation is `C:\Program Files\VMware\Orchestrator`.
   b. Set the **PATH** environment variable by pointing it to the **bin** folder of the Java JRE installed with Orchestrator.
   c. Use the Windows command prompt to navigate to the **bin** folder under the Orchestrator install folder.
      By default, the path to the **bin** folder is `C:\Program Files\VMware\Orchestrator\migration-cli\bin`.
   d. Run the export command from the command line.
      ```
      C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
      ```
      This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.
      An archive with file name `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` is created in the same folder as the migration-cli folder.

3. Import the configuration to the target Orchestrator instance.
   a. Log in to Control Center as **root**.
   b. Open **Export/Import Configuration** in Control Center and click the **Import Configuration** tab.
   c. Browse to and select the .ZIP file exported from the source Orchestrator instance.
d Enter the password that you used when exporting the configuration.
    Leave blank if you did not export the configuration with a password.

e Select the import type.

f If you are importing the configuration to an external Orchestrator server, choose whether to import the database settings.

    **Note** If the source and target Orchestrator servers are not configured to use the same external database, leave the **Migrate database settings** check box unselected to avoid upgrading the database schema to the newer version. Otherwise the source Orchestrator environment stops working.

    You must configure the database that the target Orchestrator will use before the migration.

g Click **IMPORT** to finish the migration.

    A message states that the configuration is successfully imported. The Orchestrator server service of the target Orchestrator instance restarts automatically.

4 If the target vRealize Orchestrator uses an authentication provider server that is different from the one used by the source Orchestrator, import to the trust store of the target Orchestrator the SSL certificate of the authentication provider it is configured to use.

    a On the **Certificates** page in Control Center, click **Import from URL**.

    b Provide the URL of the vRealize Automation or vSphere instance.

    A message indicates that the migration finished successfully. The Orchestrator server service restarts automatically.

**What to do next**

Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

**Migrate an External vRealize Orchestrator 6.x on Windows to vRealize Automation 7.4**

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x installed on Windows to the Orchestrator server that is built into vRealize Automation 7.4.

    **Note** If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see *Upgrading vRealize Automation* in *Installing or Upgrading vRealize Automation*.

- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.

- Stop the Orchestrator server service of the external Orchestrator.
Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1. Download the migration tool from the target Orchestrator server.
   a. Log in to the vRealize Automation appliance over SSH as root.
   b. Download the migration-tool.zip archive that is located in the /var/lib/vco/downloads directory.

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. Set the PATH environment variable by pointing it to the bin folder of the Java JRE installed with Orchestrator.
   b. Upload the migration tool to the Windows server, on which the external Orchestrator is installed.
   c. Extract the downloaded archive in the Orchestrator install folder.
      The default path to the Orchestrator install folder in a Windows-based installation is C:\Program Files\VMware\Orchestrator.
   d. Run the Windows command prompt as administrator and navigate to the bin folder in the Orchestrator install folder.
      By default, the path to the bin folder is C:\Program Files\VMware\Orchestrator\migration-cli\bin.
   e. Run the export command from the command line.

      C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export

      This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.
      The archive is created in the same folder as the migration-cli folder.

3. Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.
   a. On the vRealize Automation appliance, stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

      service vco-server stop && service vco-configurator stop

   b. Upload the exported configuration file to the /usr/lib/vco/tools/configuration-cli/bin directory on the vRealize Automation appliance.
   c. Change the ownership of the exported Orchestrator configuration file.

      chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vroat-configure` script with the `import` command.

```
./vroat-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

e Remove all certificates from the database keystore.

```
./vroat-configuration.sh untrust --reset-db
```

4 Migrate the database to the internal PostgreSQL database, by running the `vroat-configure` script with the `db-migrate` command.

```
./vroat-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Note**  Enclose passwords that contain special characters in single quotation marks.

The `JDBC_connection_URL` depends on the type of database that you use.

**PostgreSQL:** `jdbc:postgresql://host:port/database_name`


**Oracle:** `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th><code>database_name</code></th>
<th><code>vmware</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>

You successfully migrated an external vRealize Orchestrator 6.x installed on Windows to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

**What to do next**

Set up the built-in vRealize Orchestrator server. See [Configure the Built-In vRealize Orchestrator Server](#).
Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x Virtual Appliance to the Orchestrator server that is built into vRealize Automation 7.4.

Note: If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

Prerequisites

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see Upgrading vRealize Automation in Installing or Upgrading vRealize Automation.

- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.

- Stop the Orchestrator server service of the external Orchestrator.

- Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1. Download the migration tool from the target Orchestrator server to the source Orchestrator.
   a. Log in to the vRealize Orchestrator 6.x Virtual Appliance over SSH as root.
   b. Under the /var/lib/vco directory, run the scp command to download the migration-tool.zip archive.

   ```
   scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
   ```
   c. Run the unzip command to extract the migration tool archive.

   ```
   unzip migration-tool.zip
   ```

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. In the /var/lib/vco/migration-cli/bin directory, run the export command.

   ```
   ./vro-migrate.sh export
   ```

   This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.

   An archive with file name orchestrator-config-export-orchestrator_ip_address-date_hour.zip is created in the /var/lib/vco folder.
3  Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.
   a  Log in to the vRealize Automation appliance over SSH as root.
   b  Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

   ```bash
   service vco-server stop && service vco-configurator stop
   ```
   c  Under the `/usr/lib/vco/tools/configuration-cli/bin` directory, run the `scp` command to download the exported configuration archive.

   ```bash
   scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
   ```
   d  Change the ownership of the exported Orchestrator configuration file.

   ```bash
   chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
   ```
   e  Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

   ```bash
   ./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
   ```

4  If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.
   a  In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.
   b  Set the values of `listen_addresses` to a wildcard (*).

   ```bash
   listen_addresses = '*'
   ```
   c  Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.

   ```bash
   host all all vra-va-ip-address/32 md5
   ```
   **Note**  The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.
   d  Restart the PostgreSQL server service.

   ```bash
   service vpostgres restart
   ```
5 Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the \texttt{db-migrate} command.

\texttt{./vro-configure.sh db-migrate --sourceJdbcUrl JDBC\_connection\_URL --sourceDbUsername database\_user --sourceDbPassword database\_user\_password}

\textbf{Note} Enclose passwords that contain special characters in single quotation marks.

The \texttt{JDBC\_connection\_URL} depends on the type of database that you use.

- PostgreSQL: \texttt{jdbc:postgresql://host:port/database\_name}
- Oracle: \texttt{jdbc:oracle:thin:@host:port/database\_name}

The default database login information is:

<table>
<thead>
<tr>
<th>\texttt{database_name}</th>
<th>\texttt{vmware}</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{database_user}</td>
<td>\texttt{vmware}</td>
</tr>
<tr>
<td>\texttt{database_user_password}</td>
<td>\texttt{vmware}</td>
</tr>
</tbody>
</table>

6 Remove all certificates from the database keystore.

\texttt{./vro-configure.sh untrust --reset-db}

7 Reinstall the Orchestrator plug-ins.
   a Log in to Control Center as \texttt{root}.
   b Click \textbf{Troubleshooting}.
   c Click \textbf{Force plug-ins reinstall}.

8 Start the Orchestrator server service.

9 Revert to the default configuration of the \texttt{postgresql.conf} and the \texttt{pg\_hba.conf} file.
   a Restart the PostgreSQL server service.

You successfully migrated an external vRealize Orchestrator 6.x Virtual Appliance to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

\textbf{What to do next}

Set up the built-in vRealize Orchestrator server. See \textbf{Configure the Built-In vRealize Orchestrator Server}. 
Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4

You can export the configuration from your existing external Orchestrator instance and import it to the Orchestrator server that is built into vRealize Automation.

**Note** If you have multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

**Prerequisites**

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see Upgrading vRealize Automation in Installing or Upgrading vRealize Automation.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

**Procedure**

1. Export the configuration from the external Orchestrator server.
   - Log in to Control Center of the external Orchestrator server as **root** or as an **administrator**, depending on the source version.
   - Stop the Orchestrator server service from the **Startup Options** page to prevent unwanted changes to the database.
   - Go to the **Export/Import Configuration** page.
   - On the **Export Configuration** page, select **Export server configuration**, **Bundle plug-ins** and **Export plug-in configurations**.

2. Migrate the exported configuration into the embedded Orchestrator instance.
   - Upload the exported Orchestrator configuration file to the `/usr/lib/vco/tools/configuration-cli/bin` directory of the vRealize Automation appliance.
   - Log in to the vRealize Automation appliance over SSH as **root**.
   - Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

   ```
   service vco-server stop && service vco-configurator stop
   ```

   - Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

   ```
   ./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
   ```
If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.

a In the /var/vmware/vpostgres/current/pgdata/postgresql.conf file, uncomment the `listen_addresses` line.

b Set the values of `listen_addresses` to a wildcard (*).

```
listen_addresses = '*'
```

c Append a line to the /var/vmware/vpostgres/current/pgdata/pg_hba.conf file.

```
host all all vra-va-ip-address/32 md5
```

Note The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.

d Restart the PostgreSQL server service.

```
service vpostgres restart
```

Migrate the database to the internal PostgreSQL database, by running the vro-configure script with the `db-migrate` command.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

Note Enclose passwords that contain special characters in single quotation marks.

The `JDBC_connection_URL` depends on the type of database that you use.

**PostgreSQL:** `jdbc:postgresql://host:port/database_name`


**Oracle:** `jdbc:oracle:thin:@host:port/database_name`

The default database login information is:

<table>
<thead>
<tr>
<th><code>database_name</code></th>
<th><code>vmware</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database_user</code></td>
<td><code>vmware</code></td>
</tr>
<tr>
<td><code>database_user_password</code></td>
<td><code>vmware</code></td>
</tr>
</tbody>
</table>
5 Remove all certificates from the database keystore.

    ./vro-configuration.sh untrust --reset-db

6 Reinstall the Orchestrator plug-ins.
   a Log in to Control Center as root.
   b Click Troubleshooting.
   c Click Force plug-ins reinstall.

7 Start the Orchestrator server service.

8 Revert to the default configuration of the postgresql.conf and the pg_hba.conf file.
   a Restart the PostgreSQL server service.

You successfully migrated an external Orchestrator server instance to a vRealize Orchestrator instance embedded in vRealize Automation.

What to do next
Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

Configure the Built-In vRealize Orchestrator Server
After you export an external vRealize Orchestrator configuration and import it to vRealize Automation, you configure the vRealize Orchestrator server that is built into vRealize Automation.

Prerequisites
Migrate the configuration from the external to the internal vRealize Orchestrator.

Procedure
1 Log in as root to a command prompt session on the vRealize Automation appliance.
2 Start services for the vRealize Orchestrator Control Center and server:

    service vco-configurator start && service vco-server start

3 Log in as root to the built-in vRealize Orchestrator Control Center.

    https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config

   Note   You can skip the next step when the external and internal vRealize Orchestrator versions are the same.

4 In Control Center, click Validate Configuration, and verify that vRealize Orchestrator is configured properly.

5 In Control Center, click Certificates, click Package Signing Certificate, and generate a new package signing certificate.
6 In Control Center, click **Configure Authentication Provider**.

**Default tenant** and **Admin group** are set to default values `vsphere.local` and `vsphere.local\vcoadmins`. Change the defaults to the values for your environment.

7 In the vRealize Automation appliance management interface, under **Services**, verify that `vco-server` is **REGISTERED**.

8 Select the vco services of the external vRealize Orchestrator server, and click **Unregister**.

**What to do next**

- Import any certificates that were trusted in the external vRealize Orchestrator server to the trust store of the built-in vRealize Orchestrator. For more information, see [Manage Orchestrator Certificates](#).
- Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the vRealize Orchestrator configuration.
  
  For more information, see [Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability in Installing or Upgrading vRealize Automation](#).

  **Note** The vRealize Orchestrator instances are automatically clustered and available for use.

- Restart the `vco-configurator` service on all nodes in the cluster.
- Update the vRealize Orchestrator endpoint to point to the migrated built-in vRealize Orchestrator server.
- Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.

**Update Embedded vRealize Orchestrator to Trust vRealize Automation Certificates**

If you update or change vRealize Automation appliance or IaaS certificates, you must update vRealize Orchestrator to trust the new or updated certificates.

This procedure applies to all vRealize Automation deployments that use an embedded vRealize Orchestrator instance. If you use an external vRealize Orchestrator instance, see [Update External vRealize Orchestrator to Trust vRealize Automation Certificates](#).

**Note** This procedure resets tenant and group authentication back to the default settings. If you have customized your authentication configuration, note your changes so that you can re-configure authentication after completing the procedure.

See the vRealize Orchestrator documentation for information about updating and replacing vRealize Orchestrator certificates.

If you replace or update vRealize Automation certificates without completing this procedure, the vRealize Orchestrator Control Center may be inaccessible, and errors may appear in the vco-server and vco-configurator log files.

Problems with updating certificates can also occur if vRealize Orchestrator is configured to authenticate against a different tenant and group than vRealize Automation. See [https://kb.vmware.com/kb/2147612](https://kb.vmware.com/kb/2147612).
Procedure

1. Stop the vRealize Orchestrator server and Control Center services.

   ```
   service vco-server stop
   service vco-configurator stop
   ```

2. Reset the vRealize Orchestrator authentication provider.

   a. Run the `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication` command.

   b. Delete `/etc/vco/app-server/vco-registration-id`.

   c. Run `vcac-vami vco-service-reconfigure`.

3. Start the vRealize Orchestrator server and control center services.

   ```
   service vco-server start
   service vco-configurator start
   ```

Control Center Differences Between External and Embedded Orchestrator

Some of the menu items that are available in Control Center of an external vRealize Orchestrator are not included in the default Control Center view of an embedded Orchestrator instance.

In Control Center of the embedded Orchestrator server, a few options are hidden by default.

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.</td>
</tr>
<tr>
<td>Export/Import Configuration</td>
<td>The embedded Orchestrator configuration is included in the exported vRealize Automation components.</td>
</tr>
<tr>
<td>Configure Database</td>
<td>The embedded Orchestrator uses the database that is used by vRealize Automation.</td>
</tr>
<tr>
<td>Customer Experience</td>
<td>You can join the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance management interface.</td>
</tr>
<tr>
<td>Improvement Program</td>
<td>See The Customer Experience Improvement Program in Managing vRealize Automation.</td>
</tr>
</tbody>
</table>

Another options that are hidden from the default Control Center view are the **Host address** text box and the **UNREGISTER** button on the **Configure Authentication Provider** page.

**Note** To see the full set of Control Center options in vRealize Orchestrator that is built into vRealize Automation, you must access the advanced Orchestrator Management page at `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter#!/advanced` and click the F5 button on the keyboard to refresh the page.

**Reconfigure the vRealize Automation Endpoint in the Target vRealize Orchestrator**

Use the following procedure to reconfigure the vRealize Automation endpoint in the embedded target vRealize Orchestrator.
Prerequisites

- Successful migration to the latest version of vRealize Automation.
- Connect to the target vRealize Orchestrator using the vRealize Orchestrator client. For information, see Using the VMware vRealize Orchestrator Client in the vRealize Orchestrator documentation.

Procedure

1. Select Design from the top drop-down menu.
2. Click Inventory.
3. Expand vRealize Automation.
4. If you migrated from a minimal environment, identify endpoints containing the fully qualified domain name (FQDN) of the source vRealize Automation appliance host. If you migrated from a high-availability environment, identify endpoints containing the FQDN of the source appliance load balancer.

<table>
<thead>
<tr>
<th>If you find endpoints containing the FQDN, complete these steps.</th>
<th>If you do not find endpoints containing the FQDN, complete these steps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click Workflows.</td>
<td>1. Click Resources.</td>
</tr>
<tr>
<td>2. Click the expand button to select Library &gt; vRealize Automation &gt; Configuration.</td>
<td>2. Click the update icon on the top toolbar.</td>
</tr>
<tr>
<td>3. Do one of these steps.</td>
<td>3. Click the expand button to select Library &gt; vCACCAFE &gt; Configuration.</td>
</tr>
<tr>
<td>- If you migrated from a minimal environment, run the Remove a vRA host workflow for every endpoint containing the FQDN of the source vRealize Automation appliance host.</td>
<td>4. Do one of these steps.</td>
</tr>
<tr>
<td>- If you migrated from a high-availability environment, run the Remove a vRA host workflow for every endpoint containing the FQDN of the source appliance load balancer.</td>
<td>- If you migrated from a high-availability environment, delete each resource that has a URL property containing the FQDN of the source vRealize Automation appliance host.</td>
</tr>
<tr>
<td>- If you migrated from a high-availability environment, delete each resource that has a URL property containing the FQDN of the source vRealize Automation appliance load balancer.</td>
<td></td>
</tr>
</tbody>
</table>

5. Click Workflows.
6. Click the expand button to select Library > vRealize Automation > Configuration.
7. To add the target vRealize Automation appliance host or if you migrated to a high-availability deployment, the load-balanced host, run the Add a vRA host using component registry workflow.

Reconfigure the vRealize Automation Infrastructure Endpoint in the Target vRealize Orchestrator

Use the following procedure to reconfigure the vRealize Automation infrastructure endpoint in the embedded target vRealize Orchestrator.

Prerequisites

- Successful migration to the latest version of vRealize Automation.
Connect to the target vRealize Orchestrator using the vRealize Orchestrator client. For information, see *Using the VMware vRealize Orchestrator Client* in the vRealize Orchestrator documentation.

**Procedure**

1. Select **Design** from the top drop-down menu.
2. Click **Inventory**.
3. Expand **vRealize Automation Infrastructure**.
4. If you migrated from a minimal environment, identify endpoints containing the fully qualified domain name (FQDN) of the source vRealize Automation infrastructure host. If you migrated from a high-availability environment, identify endpoints containing the FQDN of the source appliance load balancer.

<table>
<thead>
<tr>
<th>If you find endpoints containing the FQDN, complete these steps.</th>
<th>If you do not find endpoints containing the FQDN, complete these steps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click <strong>Workflows</strong>. 2. Click the expand button to select <strong>Library &gt; vRealize Automation &gt; Infrastructure Administration &gt; Configuration</strong>. 3. Do one of these steps.</td>
<td>1. Click <strong>Resources</strong>. 2. Click the update icon on the top toolbar. 3. Click the expand button to select <strong>Library &gt; vCAC &gt; Configuration</strong>. 4. Do one of these steps.</td>
</tr>
</tbody>
</table>
| - If you migrated from a minimal environment, run the **Remove an IaaS host** workflow for every endpoint containing the FQDN of the source vRealize Automation infrastructure host.  
- If you migrated from a high-availability environment, run the **Remove an IaaS host** workflow for every endpoint containing the FQDN of the source vRealize Automation infrastructure host load balancer. | - If you migrated from a minimal environment, delete each resource that has a host property containing the FQDN of the source vRealize Automation infrastructure host.  
- If you migrated from a high-availability environment, delete each resource that has a host property containing the FQDN of the source vRealize Automation infrastructure host load balancer. |

5. Click **Workflows**.
6. Click the expand button to select **Library > vRealize Automation > Configuration**.
7. To add the target vRealize Automation infrastructure host, or if you migrated to a high-availability deployment load-balanced host, run the **Add the IaaS host of a vRA host** workflow.

**Install vRealize Orchestrator Customization**

You can run a workflow to install the customized state change workflow stubs and vRealize Orchestrator menu operation workflows.

For information, see *Install vRealize Orchestrator Customization*.

**Prerequisites**

Successful migration to the latest version of vRealize Automation.
Reconfigure Embedded vRealize Orchestrator Infrastructure Endpoint in the Target vRealize Automation

When you migrate from a vRealize Automation 6.2.x environment, you must update the URL of the infrastructure endpoint that points to the target embedded vRealize Orchestrator server.

Prerequisites

- Successfully migrate to vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  
  a Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.
  
  For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.
  
  b Log in as a IaaS administrator user.

Procedure

1. Select Infrastructure > Endpoints > Endpoints.
2. On the Endpoints page, select the vRealize Orchestrator endpoint, and click Edit.
3. In the Address text box, edit the vRealize Orchestrator endpoint URL.
   
   a If you migrated to a minimal environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-hostname.domain.name:443/vco.
   
   b If you migrated to a high-availability environment, replace the vRealize Orchestrator endpoint URL with https://vra-va-lb-hostname.domain.name:443/vco.
4. Click OK.
5. Manually run a data collection on the vRealize Orchestrator endpoint.
   
   a On the Endpoints page, select the vRealize Orchestrator endpoint.
   
   b Select Actions > Data Collection.
   
   Verify that the data collection is successful.

Reconfigure the Azure Endpoint in the Target vRealize Automation Environment

After migration, you must reconfigure your Microsoft Azure endpoint.

Perform this procedure for each Azure endpoint.

Prerequisites

- Successfully migrate to the latest version of vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  
  a Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.
For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.

b Log in as a IaaS administrator user.

Procedure
1 Select Administration > vRO Configuration > Endpoints.
2 Select an Azure endpoint.
3 Click Edit.
4 Click Details.
5 In the Client secret text box, enter the original client secret.
6 Click Finish.
7 Repeat for each Azure endpoint.

Migrate vRealize Automation 6.2.x Automation Application Services to 7.4
You can use the VMware vRealize Application Services Migration Tool to migrate your existing application services blueprints and deployment profiles from VMware vRealize Application Services 6.2.x to vRealize Automation 7.4.

Prerequisites
Successful migration to the latest version of vRealize Automation.

Procedure
To download the VMware vRealize Application Services Migration Tool, complete these steps.

a Click Download VMware vRealize Automation.

b Select Drivers & Tools > VMware vRealize Application Services Migration Tool.

Delete Original Target vRealize Automation IaaS Microsoft SQL Database
You can delete the original IaaS database after migration is complete.

Prerequisites
Successful migration to the latest version of vRealize Automation.

Your migrated environment does not use the original vRealize Automation IaaS Microsoft SQL database that you created when you installed the target vRealize Automation environment. You can safely delete this original IaaS database from the Microsoft SQL Server after you complete migration.

Update Data Center Location Menu Contents After Migration
After migration, you must add any missing custom data center locations to the Location drop-down menu.
After migration to the latest version of vRealize Automation, the data center locations in the Location drop-down menu on the Compute Resources page revert to the default list. Although custom data center locations are missing, all compute resource configurations migrate successfully and the Vrm.DataCenter.Location property is not affected. You can still add custom data center locations to the Location menu.

**Prerequisites**

Migrate to the latest version of vRealize Automation.

**Procedure**

- Add missing data center locations to the Location drop-down menu. See Scenario: Add Datacenter Locations for Cross Region Deployments.

**Upgrading Software Agents to TLS 1.2**

After you migrate to vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4, you must perform several tasks to upgrade the Software Agents from your source environment to Transport Layer Security (TLS) 1.2. Beginning with vRealize Automation 7.4, TLS 1.2 is the only supported TLS protocol for data communication between vRealize Automation and your browser. After migration, you must upgrade existing virtual machine templates from your vRealize Automation 7.1 or 7.3 source environment as well as any existing virtual machines.

**Update Source Environment Virtual Machine Templates**

You must update existing vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 templates after you complete migration to 7.4 so that the Software Agents use the TLS 1.2 protocol.

Guest agent and agent bootstrap code must be updated in the source environment templates. If you are using a linked clone option, you might need to remap the templates with the newly created virtual machines and their snapshots.

To upgrade your templates, you complete these tasks.

1. Log in to vSphere.
2. Convert each template from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to a virtual machine and power on the machine.
3. Import the appropriate software installer and run the software installer on each virtual machine.
4. Convert each virtual machine back to a template.

Use this procedure to locate the software installers for Linux or Windows.

**Prerequisites**

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
Procedure

1. Start a browser and open the vRealize Automation 7.4 appliance splash page using the fully qualified domain name of the virtual appliance: https://vra-va-hostname.domain.name.

2. Click Guest and software agents page.

3. Follow the instructions for the Linux or Windows software installers.

What to do next

Identify Virtual Machines that Need Software Agent Upgrade.

Identify Virtual Machines that Need Software Agent Upgrade

You can use the Health Service in the vRealize Automation Console to identify virtual machines that need software agent update to TLS 1.2.

Sometimes the patch applied to your vRealize Automation source environment does not upgrade all of the virtual machines. You can use the Health Service to identify the virtual machines that still need a software agent update to TLS 1.2. All software agents in the target environment need to be updated for post-provisioning procedures.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- You have successfully migrated vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You are logged in to vRealize Automation 7.4 on the primary virtual appliance.

Procedure

1. Click Administration > Health.

2. Click New Configuration.

3. On the Configuration Details page, provide the requested information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter SW Agent verification</td>
</tr>
<tr>
<td>Description</td>
<td>Add optional description, for example,</td>
</tr>
<tr>
<td></td>
<td>Locate software agents for upgrade to TLS 1.2</td>
</tr>
<tr>
<td>Product</td>
<td>Select vRealize Automation 7.4.0.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Select None.</td>
</tr>
</tbody>
</table>

4. Click Next.


6. Click Next.
On the Configure Parameters page, provide the requested information.

### Table 1-101. vRealize Automation Virtual Appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Public Web Server Address     | - For a minimal deployment, the base URL for the vRealize Automation appliance host. For example, https://va-host.domain/.
|                               | - For a high-availability deployment, the base URL for the vRealize Automation load balancer. For example, https://load-balancer-host.domain/.
| SSH Console Address           | Fully qualified domain name of the vRealize Automation appliance. For example, va-host.domain. |
| SSH Console User              | root                                                                        |
| SSH Console Password          | Password for root.                                                         |
| Max Service Response Time (ms)| Accept default: 2000                                                        |

### Table 1-102. vRealize Automation System Tenant

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tenant Administrator</td>
<td>administrator</td>
</tr>
<tr>
<td>System Tenant Password</td>
<td>Password for administrator.</td>
</tr>
</tbody>
</table>

### Table 1-103. vRealize Automation Disk Space Monitoring

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning Threshold Percent</td>
<td>Accept default: 75</td>
</tr>
<tr>
<td>Critical Threshold Percent</td>
<td>Accept default: 90</td>
</tr>
</tbody>
</table>

### Table 1-104. vRealize Automation Tenant

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant Under Test</td>
<td>Tenant selected for testing.</td>
</tr>
<tr>
<td>Fabric Administrator User Name</td>
<td>Fabric administrator user name. For example, <a href="mailto:admin@va-host.local">admin@va-host.local</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This fabric administrator must also have a tenant administrator and an IaaS administrator role in order for all of the tests to run.</td>
</tr>
<tr>
<td>Fabric Administrator Password</td>
<td>Password for fabric administrator.</td>
</tr>
</tbody>
</table>

Click **Next**.

On the Summary page, review the information and click **Finish**.

The software agent verification configuration is finished.

On the SW Agent verification card, click **Run**.

When the test is complete, click the center of the SW Agent verification card.
12 On the SW Agent verification results page, page through the test results and find the Check Software Agent Version test in the Name column. If the test result is Failed, click the Cause link in the Cause column to see the virtual machines with an outdated software agent.

What to do next

If you have virtual machines with an outdated software agent, see Upgrade Software Agents on vSphere.

Upgrade Software Agents on vSphere

You can upgrade any outdated Software Agents on vSphere to TLS 1.2 after migration using vRealize Automation Appliance Management.

This procedure updates the outdated Software Agents on the virtual machines from your source environment to TLS 1.2 and is required for migration to vRealize Automation 7.4.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You have used Health Service to identify virtual appliances with outdated Software Agents.

Procedure

1 On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as root using the password you entered when you deployed the vRealize Automation appliance.

   For a high-availability environment, open Appliance Management on the master appliance.

2 Click vRA Settings > SW Agents.

3 Click Toggle TLS 1.0, 1.1.

   TLS v1.0, v1.1 Status is ENABLED.

4 For Tenant credentials, enter the requested information for the source vRealize Automation appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant name</td>
<td>Name of tenant on the source vRealize Automation appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The tenant user must have the Software Architect role assigned.</td>
</tr>
<tr>
<td>Username</td>
<td>Tenant administrator user name on the source vRealize Automation appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>Tenant administrator password.</td>
</tr>
</tbody>
</table>

5 Click Test connection.

   If a connection is established, a success message appears.
6 For Source appliance, enter the IP address or fully qualified domain name of the source vRealize Automation appliance.

The source and the target appliance must both use the same tenant credentials.

7 Click **List batches**.

The Batch Choice List table appears.

8 Click **Show**.

A table appears with a list of virtual machines with outdated Software Agents.

9 Upgrade the Software Agent for the virtual machines that are in the UPGRADABLE state.

- To upgrade the Software Agent in an individual virtual machine, click **Show** for a group of virtual machines, identify the virtual machine you want to upgrade and click **Run** to start the upgrade process.

- To upgrade the Software Agent for a batch of virtual machines, identify the group that you want to upgrade and click **Run** to start the upgrade process.

If you have more than 200 virtual machines to upgrade, you can control the batch upgrade process speed by entering values for these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Queue Depth</td>
<td>The number of parallel upgrade executions that take place at one time. For example, 20. You can vary this number to adjust the upgrade speed.</td>
</tr>
<tr>
<td>Batch Errors</td>
<td>The REST error count causing batch upgrade to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Failures</td>
<td>The number of failed Software Agent upgrades causing batch processing to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.</td>
</tr>
<tr>
<td>Batch Polling</td>
<td>How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.</td>
</tr>
</tbody>
</table>

If the upgrade process is too slow or produces too many unsuccessful upgrades, you can adjust these parameters to improve upgrade performance.

**Note** Clicking **Refresh** clears the list of batches. It does not affect the upgrade process. It also refreshes information about whether TLS 1.2 is set or not. In addition, clicking **Refresh** also performs a health check of vRealize Automation services. If services are not running, the system displays an error message and inactivates all other action buttons.
Click **Toggle TLS 1.0, 1.1.**

**TLS v1.0, v1.1 Status is DISABLED.**

**Upgrade Software Agents on Amazon Web Service or Azure**

You can upgrade outdated Software Agents on Amazon Web Service (AWS) or Azure manually.

- You must update the tunnel properties specified in the reservation of the migrated vRealize Automation server.

**Prerequisites**

- **Apply Software Agent Patch** if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- A software tunnel is present and the tunnel virtual machine IP address is known.

**Procedure**

1. Create a node file for each node that you need to upgrade.

   ```
   /usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
   ```

2. Create a plan file to upgrade the Software Agent on a Linux or a Windows virtual machine.

   - Modify the migrate params file under `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` to contain the value of the private IP address corresponding to the AWS or Azure endpoint.

     ```
     "key": "ipAddress",
     "value": {
       "type": "string",
       "value": "<$PrivateIp:$PrivatePort>"
     }
     ```

   - Use this command for updating a Linux machine.

     ```
     ```

   - Use this command for updating a Windows machine.

     ```
     ```
This command runs the plan file.

```bash
```

3 Use this command to update the Software Agent using the node file from step 1 and the plan file from step 2.

```bash
```

As an alternative, you can use this command to run one node at a time from the node file by providing a node index.

```bash
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

As you perform this procedure, you can tail logs from the vRealize Automation virtual appliance and host machine to see the Server Agent upgrade process.

After upgrade, the upgrade process imports a software update script for Windows or Linux to the vRealize Automation 7.4 virtual appliance. You can log into the vRealize Automation virtual appliance host to ensure that the software component is imported successfully. After the component is imported, a software update is sent to the old Event Broker Service (EBS) to relay software update scripts to the identified virtual machines. When the upgrade completes and the new Software Agents become operative, they bind to the new vRealize Automation virtual appliance by sending a ping request.

**Note** Useful Log Files

- Catalina output for source vRealize Automation: /var/log/vcac/catalina.out. In this file, you see the upgrade requests being made as the agent migrations are made. This activity is the same as running a software provisioning request.

- Catalina output for destination vRealize Automation: /var/log/vcac/catalina.out. In this file, you see the migrated virtual machines reporting their ping requests here to include version numbers 7.4.0-SNAPSHOT. You can tally these together by comparing the EBS topic names, for example, sw-agent-UUID.

- Agent update folder on destination vRealize Automation machine master upgrade log file: /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. You can tail this file to see which upgrade operation is in progress.
Individual logs available under tenant folders: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Individual nodes are listed here as lot files with failures and in-progress extensions.

Migrated VMs: `/opt/vmware-appdirector/agent/logs/darwin*.log`. You can spot check this location which should list the software update requests being received as well as the eventual restart of the agent_bootstrap + software agent.

Change Property Dictionary Setting After Migration from 6.2.5

The `Label` control in the vRealize Automation 6.2.x property dictionary does not exist in the vRealize Automation 7.x property dictionary.

During migration to vRealize Automation 7.4 or earlier, the `Label` control is converted to a `TextBox` control type in the migrated property dictionary.

During migration to vRealize Automation 7.5 or later, the `Label` control is converted to a `TextArea` control type in the migrated property dictionary. The `TextArea` control type supports long label names better than the `TextBox` control type used when migrating to earlier versions of vRealize Automation 7.x.

After migration, you can set property definitions that contain an impacted `TextBox` or `TextArea` control type as not overridable, either manually in each blueprint's vRealize Automation properties settings, manually in each blueprint component, reservation, endpoint and so on in which an impacted custom property definition is used, or programmatically by using export and import capabilities in vRealize CloudClient.

Procedure

1. After migration and to determine which property definitions use a `TextBox` (7.4 and earlier) or `TextArea` (7.5 or later) type control, click `Administration > Property Definitions` and view the `Display Area` setting for each property definition of the `String` data type.

   These are the property definitions to set as not overrideable in your migrated vRealize Automation instance.

2. Set impacted custom properties as not overrideable.
   - Manually for the overall blueprint
     1. Click the `Design` tab and open a blueprint.
     2. Click the gear icon to open the `Blueprint Properties` page.

   3. Click the `Properties` tab on the `Blueprint Properties` page and click `Custom Properties`.
   4. Toggle `Overrideable` off for all property definitions that contain a `TextBox` or `TextArea` control type.

   - Manually for each blueprint component, reservation, endpoint and so on in which an impacted custom property is used
     1. For endpoints and reservation, click `Infrastructure` and select either `Endpoints` or `Reservations`. 
2 Open each target element and use its Properties tab to set the impacted TextBox (7.4 and earlier) or TextArea (7.5 or later) type control as not overrideable.

3 Open each blueprint and use the Properties tab in each machine, network, and other component in the blueprint canvas to update any impacted property definitions.

- Programmatically for the overall blueprint
  1 Export the blueprint by using a vRealize CloudClient export command sequence.
  2 Mark the impacted property definitions as not overrideable. In this example, TestLabel is set to not overridable and TestOverrideLabel is set in a way that it can be edited on a request form.

```
TestLabel:
  fixed: default test label description at BP
  required: true
  secured: false
  visible: true
TestOverrideLabel:
  default: override this value
  required: true
  secured: false
  visible: true
```

3 Import the blueprint by using a vRealize CloudClient import command sequence.

 validates the Target vRealize Automation 7.4 Environment

You can verify that all data is migrated successfully to the target vRealize Automation environment.

Prerequisites

- Migrate to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console.
  a  Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://vra-va-hostname.domain.name/vcac.

For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://vra-va-lb-hostname.domain.name/vcac.
  b  Log in with the tenant administrator user name and password.

Procedure

1 Select Infrastructure > Managed Machines and verify that all the managed virtual machines are present.

2 Click Compute Resources, select each endpoint, and click Data Collection, Request now, and Refresh to verify that the endpoints are working.

3 Click Design, and on the Blueprints page, verify the elements of each blueprint.
4 Click XaaS and verify the contents of Custom Resources, Resource Mappings, XaaS Blueprints, and Resource Actions.

5 Select Administration > Catalog Management and verify the contents of Services, Catalog Items, Actions, and Entitlements.

6 Select Items > Deployments and verify the details for the provisioned virtual machines.

7 On the Deployments page, select a provisioned, powered off, virtual machine and select Actions > Power On, click Submit, and click OK. Verify that the virtual machine powers on correctly.

8 Click Catalog and request a new catalog item.

9 On the General tab, enter the request information.

10 Click the Machine icon, accept all the default settings, click Submit, and click OK.

11 Verify that the request finishes successfully.

**Troubleshooting Migration**

Migration troubleshooting topics provide solutions to problems you might experience when you migrate vRealize Automation.

**PostgreSQL Version Causes Error**

A source vRealize Automation 6.2.x environment containing an updated PostgreSQL database blocks administrator access.

**Problem**

If an upgraded PostgreSQL database is used by vRealize Automation 6.2.x, an administrator must add an entry to the pg_hba.conf file that provides access to this database from vRealize Automation.

**Solution**

1 Open the pg_hba.conf file.

2 To grant access to this database, add the following entry.

   ```
   host all vcac-database-user vra-va-ip trust-method
   ```

**Some Virtual Machines Do Not Have a Deployment Created during Migration**

Virtual machines in the missing state at the time of migration do not have a corresponding deployment created in the target environment.

**Problem**

If a virtual machine is in the missing state in the source environment during migration, a corresponding deployment is not created in the target environment.

**Solution**

- If a virtual machine goes out of the missing state after migration, you can import the virtual machine to the target deployment using bulk import.
Migration Log Locations
You can troubleshoot validation or migration problems by viewing the logs that record the migration process.

Table 1-105. Source vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package creation log</td>
<td>/var/log/vmware/vcac/migration-package.log</td>
</tr>
</tbody>
</table>

Table 1-106. Target vRealize Automation Appliance

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration log</td>
<td>/var/log/vmware/vcac/migrate.log</td>
</tr>
<tr>
<td>Migration execution log</td>
<td>/var/log/vmware/vcac/mseq.migration.log</td>
</tr>
<tr>
<td>Migration execution output log</td>
<td>/var/log/vmware/vcac/mseq.migration.out.log</td>
</tr>
<tr>
<td>Validation execution log</td>
<td>/var/log/vmware/vcac/mseq.validation.log</td>
</tr>
<tr>
<td>Validation execution output log</td>
<td>/var/log/vmware/vcac/mseq.validation.out.log</td>
</tr>
</tbody>
</table>

Table 1-107. Target vRealize Automation Infrastructure Nodes

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration log</td>
<td>C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log</td>
</tr>
<tr>
<td>Validation log</td>
<td>C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log</td>
</tr>
</tbody>
</table>

Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request
Catalog items that use certain property definitions from prior versions appear in the service catalog but are not available to request after migrating to the latest version of vRealize Automation.

Problem
If you migrated from a 6.2.x or earlier version and you had property definitions with these control types or attributes, these elements are missing from the property definitions and any catalog items that use the definitions do not function as they did before you performed the migration.

- Control types. Check box or link.
- Attributes. Relationship, regular expressions, or property layouts.

Cause
In vRealize Automation 7.0 and later, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes.

Migrate the control type or attributes to vRealize Automation 7.x using a script action.
Solution

1. In vRealize Orchestrator, create a script action that returns the property values. The action must return a simple type. For example, return strings, integers, or other supported types. The action can take the other properties on which it depends as an input parameter.

2. In vRealize Automation console, configure the product definition.
   b. Select the property definition and click Edit.
   c. From the Display advice drop-down menu, select Dropdown.
   d. From the Values drop-down menu, select External Values.
   e. Select the script action.
   f. Click OK.
   g. Configure the Input Parameters that are included in the script action. To preserve the existing relationship, bind the parameter to the other property.
   h. Click OK.

Data Collection Radio buttons Disabled in vRealize Automation

After migration from vRealize Automation 6.2.x to 7.x, the Compute Resources page on the target vRealize Automation contains disabled radio buttons under Data Collection.

Cause

If you install an agent on the source environment that points to an endpoint and install an agent on the target environment that points to the same endpoint but the agent has a different name, you can run a test connection to the endpoint as administrator in the target environment. However, if you log in to vRealize Automation on the target environment as a fabric administrator, the radio buttons on the Compute Resources page under Data Collection are disabled.

Solution

Avoid this situation by giving the name of the agent installed on the target environment the same name as the agent installed on the source environment.

Troubleshooting the Software Agent Upgrade

When you use vRealize Automation Appliance Management to upgrade software agents, you can review log files to identify the cause of any problems you experience.
Problem

You might experience problems when you upgrade the software agents. By observing the log files during the software agent upgrade process, you can identify where there is a problem.

Note  Server Logs

- Tail the updateSoftwareAgents.log file on the server to observe the process: /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log.
- Tail the catlaina.out file on target appliance to see which software agents are succeeding: /var/log/vcac/catalina.out.

  Look for a string such as "ping" reported back for 7.4.0-SNAPSHOT.

You can find additional information at these locations.

- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan
- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log
- /var/cache/vcac/agentupdate/sqa/UUID/UUID.log (per OS)

Before you start a major batch upgrade, you should always perform a test virtual appliance software agent upgrade. For an overview of the process:

- Observe the first request made to the target virtual appliance to identify the agent versions.
- Observe the request made to the source virtual appliance for upgrade.
- Observe the agents reporting their new 7.4 version in the target virtual appliance.
- Between these events, observe the updateSoftwareAgents.log file at /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log

Note  Client Logs

Linux agent logs are in appdirector agent logs folder: /opt/vmware-appdirector/agent/logs/*.log

You might see log errors like these, which are temporary because the EBS queues go out and in during the upgrade process.


org.springframework.web.client.HttpClientErrorException: 404 Not Found

at org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]
Installing and Upgrading vRealize Automation

at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[noble-agent.jar:na]
at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[noble-agent.jar:na]
at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[noble-agent.jar:na]
at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler$EventPoller.run(RestEventSubscribeHandler.java:329) ~[noble-agent.jar:na]