Upgrading from vRealize Automation 7.1 or Later to 7.4

16 January 2019
vRealize Automation 7.4

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Updated Information

The following table lists the changes to *Upgrading from vRealize Automation 7.1 or Later to 7.4* for this product release.

Revision	Description
16 JAN 2019	Minor updates.
17 DEC 2018	Removed a topic that did not apply to upgrade from 7.1 or later.
16 NOV 2018	Minor updates.
05 OCT 2018	Minor updates.
15 JUN 2018	■ Clarified login information in Replica vRealize Automation Appliance Fails to Update. ■ Added a KB reference to Downloading vRealize Automation Appliance Updates.
3 MAY 2018	■ Revised Exclude IaaS Upgrade. ■ Revised Work Around Upgrade Problems. ■ Revised Upgrading a Stand-Alone vRealize Orchestrator Appliance for Use with vRealize Automation.
12 APR 2018	Initial document release.

Upgrading vRealize Automation 7.1, 7.2, or 7.3.x to 7.4

1

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 lunger 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.

This chapter includes the following topics:

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* in Reference Architecture in the vRealize Automation documentation.

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 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 1-1. Checklist for Upgrading a vRealize Automation Minimal Environment

Task	Instructions
❑ Run NSX Network and Security Inventory Data Collection Before You Upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4. This is only required when vRealize Automation is integrated with NSX.	See Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.
❑ Backup your current installation. This is a critical step.	For more information on how to back up and restore your system, see Back Up Your Existing vRealize Automation Environment. For general information, see *Configuring Backup and Restore by Using Symantec Netbackup* at http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf.

Table 1-1. Checklist for Upgrading a vRealize Automation Minimal Environment (Continued)

Task	Instructions
❑ Download update to the vRealize Automation appliance.	See Downloading vRealize Automation Appliance Updates.
❑ Install the update on the vRealize Automation appliance and IaaS components.	See Install the Update on the vRealize Automation Appliance and IaaS Components

Table 1-2. Checklist for Upgrading a vRealize Automation Distributed Environment

Task	Instructions
❑ Run NSX Network and Security Inventory Data Collection Before You Upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4. This is only required when vRealize Automation is integrated with NSX.	See Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.
❑ Back up your current installation. This is a critical step.	For more information on how to back up and restore your system, see Back Up Your Existing vRealize Automation Environment. For detailed information, see *Configuring Backup and Restore by Using Symantec Netbackup* at http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf
❑ If you are upgrading from vRealize Automation 7.3.x, disable the PostgreSQL automatic failover.	See Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.
❑ Download updates to the vRealize Automation appliance.	See Downloading vRealize Automation Appliance Updates.
❑ Disable your load balancer.	See your load balancer documentation.
❑ Install the update on the master vRealize Automation appliance and IaaS components. **Note** You must install the update on the master appliance in a distributed environment..	See Install the Update on the vRealize Automation Appliance and IaaS Components.
❑ Enable your load balancer.	Chapter 7 Enable Your Load Balancers

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 1-3. vRealize Automation Administration Console

Purpose	Access	Required Credentials
You use the vRealize Automation console for these system administrator tasks. ■ Add tenants. ■ Customize the vRealize Automation user interface. ■ Configure email servers. ■ View event logs. ■ Configure vRealize Orchestrator.	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**. You can also use this URL to open the vRealize Automation console: https://*vra-va-hostname.domain.name*/vcac 3 Log in.	You must be a user with the system administrator role.

Table 1-4. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

Purpose	Access	Required Credentials
You use vRealize Automation for these tasks. ■ Request new IT service blueprints. ■ Create and manage cloud and IT resources. ■ Create and manage custom groups. ■ Create and manage business groups. ■ Assign roles to users.	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/org/*tenant_URL_name* . 2 Log in.	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

Table 1-5. vRealize Automation Appliance Management. This interface is sometimes called the Virtual Appliance Management Interface (VAMI).

Purpose	Access	Required Credentials
You use vRealize Automation Appliance Management for these tasks. ■ View the status of registered services. ■ View system information and reboot or shutdown the appliance. ■ 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.	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.	■ User name: root ■ Password: Password you entered when you deployed the vRealize Automation appliance.

Table 1-6. vRealize Orchestrator Client

Purpose	Access	Required Credentials
You use the vRealize Orchestrator Client for these tasks. ■ Develop actions. ■ Develop workflows. ■ Manage policies. ■ Install packages. ■ Manage user and user group permissions. ■ Attach tags to URI objects. ■ View inventory.	1 Start a browser and open the vRealize Automation splash page using the fully qualified domain name of the virtual appliance: https://*vra-va-hostname.domain.name*. 2 To download the client.jnlp file to your local computer, click **vRealize Orchestrator Client**. 3 Right-click the `client.jnlp` file and select **Launch**. 4 On the Do you want to Continue? dialog box, click **Continue**. 5 Log in.	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.

Table 1-7. vRealize Orchestrator Control Center

Purpose	Access	Required Credentials
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 1-8. Linux Command Prompt

Purpose	Access	Required Credentials
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 1-9. Windows Command Prompt

Purpose	Access	Required Credentials
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

2

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.

4 Upgrade VMware vRealize Business for Cloud.

This section provides additional guidance for managing vRealize Business for Cloud when it is integrated with your vRealize Automation environment.

This chapter includes the following topics:

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

1. Unregister vRealize Business for Cloud from vRealize Automation. See *Unregister vRealize Business for Cloud from vRealize Automation* in the vRealize Business for Cloud Documentation.
2. Upgrade vRealize Automation.
3. If necessary, upgrade vRealize Business for Cloud for Cloud. See *Upgrading vRealize Business for Cloud* in the vRealize Business for Cloud Documentation.
4. Register vRealize Business for Cloud with vRealize Automation. See *Register vRealize Business for Cloud with vRealize Automation* in the vRealize Business for Cloud Documentation.

Preparing to Upgrade vRealize Automation

3

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.

This chapter includes the following topics:

- Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation
- Backup Prerequisites for Upgrading vRealize Automation
- Back Up Your Existing vRealize Automation Environment
- Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous
- Downloading vRealize Automation Appliance Updates

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* in *Managing vRealize Automation*.

What to do next

Backup Prerequisites for Upgrading vRealize Automation.

Backup Prerequisites for Upgrading vRealize Automation

Complete the backup prerequisites before you upgrade vRealize Automation 7.1, 7.2, or 7.3.x to 7.4.

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/`
  - `/etc/rabbitmq/`
- 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* in *Managing vRealize Automation*.

What to do next

Back Up Your Existing vRealize Automation Environment.

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* in *Managing vRealize Automation*.

Prerequisites

- Backup Prerequisites for Upgrading vRealize Automation.
- 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 (xmldb) 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* in the *Managing vRealize Automation* PDF in vRealize Automation product documentation.
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* in the *Managing vRealize Automation* PDF in vRealize Automation product documentation.
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-va-hostname.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 envrionment.
- 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.
   a. Start a browser and go to the vRealize Automation product page at www.vmware.com.
   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

4

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 update 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 Automationand 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 Chapter 9 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.

d 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.

For more information about the Customer Experience Improvement Program, see *Join or Leave the Customer Experience Improvement Program for vRealize Automation* in *Managing 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 Chapter 5 Upgrading the IaaS Server Components Separately If the Update Process Fails.

Upgrading the IaaS Server Components Separately If the Update Process Fails

5

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.

This chapter includes the following topics:

- Upgrade IaaS Components Using the Upgrade Shell Script After Upgrading the vRealize Automation Appliance
- Upgrading IaaS Components Using the IaaS Installer Executable File After Upgrading the vRealize Automation Appliance
- Restore Access to the Built-In vRealize Orchestrator Control Center

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 Chapter 9 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 Chapter 4 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 the vRealize Automation Appliance.

Upgrade the IaaS Components After Upgrading the vRealize Automation Appliance

After you upgrade the vRealize Automation Appliance to 7.4, you must upgrade the PostgreSQL database and configure all systems that have IaaS components installed. You can use this procedure 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 161 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.

Option	Action
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. 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.
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. 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 *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 of the services that you upgrade run under this account.
To specify your Microsoft SQL Server database	If you are upgrading the Model Manager Data, enter the names of the database server and database instance in the **Server** 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 **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, uncheck **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 recommended 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.

17 (Optional) Enable Automatic Manager Service Failover. See *Enable Automatic Manager Service Failover* in *Installing vRealize Automation*.

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, re-enable the vRealize Automation health monitors and the traffic to all 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.

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 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.

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

Chapter 6 Upgrading vRealize Orchestrator After Upgrading vRealize Automation.

Upgrading vRealize Orchestrator After Upgrading vRealize Automation

6

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.

This chapter includes the following topics:

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.

Menu Item	Details
Licensing	The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.
Export/Import Configuration	The embedded Orchestrator configuration is included in the exported vRealize Automation components.
Configure Database	The embedded Orchestrator uses the database that is used by vRealize Automation.
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 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.

      ```
      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.

      ```
      ./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
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

The default database login information is:

database_name	vmware
database_user	vmware
database_user_password	vmware

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.

5 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 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.
- 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 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.
- 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 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.
- 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`*`-updaterepo.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.

   `http://`*`local_web_server`*`:`*`port`*`/build/mts/release/bora-`*`build_number`*`/publish/exports/Update_Repo`
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 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.

2 Upgrade only one of the Orchestrator server instances in your cluster using one of the documented procedures.

3 Deploy a new Orchestrator appliance on version 7.3.
   a Configure the new node with the network settings of an existing not upgraded instance that is part of the cluster.
4 Access Control Center of the second node to start the configuration wizard.
   a Navigate to https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter.
   b Log in as **root** with the password you entered during OVA deployment.
5 Select the **Clustered Orchestrator** deployment type.

   By choosing this type, you select to join the node to an existing Orchestrator cluster.
6 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.
7 In the **User name** and **Password** text boxes, enter the root credentials of the first Orchestrator server instance.
8 Click **Join**. The Orchestrator instance clones the configuration of the node, to which it joins.

   The Orchestrator server service of both nodes restart automatically.
9 Access Control Center of the upgraded Orchestrator cluster through the load balancer address and log in as an **administrator**.
10 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.
11 Verify that the vRealize Orchestrator cluster is configured properly by opening the **Validate Configuration** page in Control Center.
12 (Optional) Repeat steps 3 through 8 for each additional node in the cluster.

You have successfully upgraded the Orchestrator cluster.

What to do next

Chapter 7 Enable Your Load Balancers.

Migrating vRealize Automation

You can perform a side-by-side upgrade of your current vRealize Automation environment to the latest version of vRealize Automation by using migration.

Updated Information

This *Migrating vRealize Automation* is updated with each release of the product or when necessary.

This table provides the update history of *Migrating vRealize Automation*.

Revision	Description
13 NOV 2018	Updated Change Property Dictionary Setting After Migration from 6.2.5.
04 OCT 2018	Minor updates.
20 SEP 2018	Initial release.

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 the VMware vRealize Application Services integration that was supported in vRealize Automation 6.2.5.

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 6.2.5, you might experience these issues.

Issue	Resolution
After you migrate from vRealize Automation 6.2.5 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 the vRealize Automation release, 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.
Regular expressions used to define the parent-child relationships in a vRealize Automation 6.2.5 drop-down menu are not supported in the target vRealize Automation release. In 6.2.5, 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, 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."	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 6-1. vRealize Automation Administration Console

Purpose	Access	Required Credentials
You use the vRealize Automation console for these system administrator tasks. ■ Add tenants. ■ Customize the vRealize Automation user interface. ■ Configure email servers. ■ View event logs. ■ Configure vRealize Orchestrator.	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**. You can also use this URL to open the vRealize Automation console: https://*vra-va-hostname.domain.name*/vcac 3 Log in.	You must be a user with the system administrator role.

Table 6-2. vRealize Automation Tenant Console. This interface is the primary user interface that you use to create and manage your services and resources.

Purpose	Access	Required Credentials
You use vRealize Automation for these tasks. ■ Request new IT service blueprints. ■ Create and manage cloud and IT resources. ■ Create and manage custom groups. ■ Create and manage business groups. ■ Assign roles to users.	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/org/*tenant_URL_name* . 2 Log in.	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

Table 6-3. vRealize Automation Appliance Management. This interface is sometimes called the Virtual Appliance Management Interface (VAMI).

Purpose	Access	Required Credentials
You use vRealize Automation Appliance Management for these tasks. ■ View the status of registered services. ■ View system information and reboot or shutdown the appliance. ■ 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.	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.	■ User name: root ■ Password: Password you entered when you deployed the vRealize Automation appliance.

Table 6-4. vRealize Orchestrator Client

Purpose	Access	Required Credentials
You use the vRealize Orchestrator Client for these tasks. ■ Develop actions. ■ Develop workflows. ■ Manage policies. ■ Install packages. ■ Manage user and user group permissions. ■ Attach tags to URI objects. ■ View inventory.	1 Start a browser and open the vRealize Automation splash page using the fully qualified domain name of the virtual appliance: https://*vra-va-hostname.domain.name*. 2 To download the client.jnlp file to your local computer, click **vRealize Orchestrator Client**. 3 Right-click the `client.jnlp` file and select **Launch**. 4 On the Do you want to Continue? dialog box, click **Continue**. 5 Log in.	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.

Table 6-5. vRealize Orchestrator Control Center

Purpose	Access	Required Credentials
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 6-6. Linux Command Prompt

Purpose	Access	Required Credentials
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 6-7. Windows Command Prompt

Purpose	Access	Required Credentials
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.

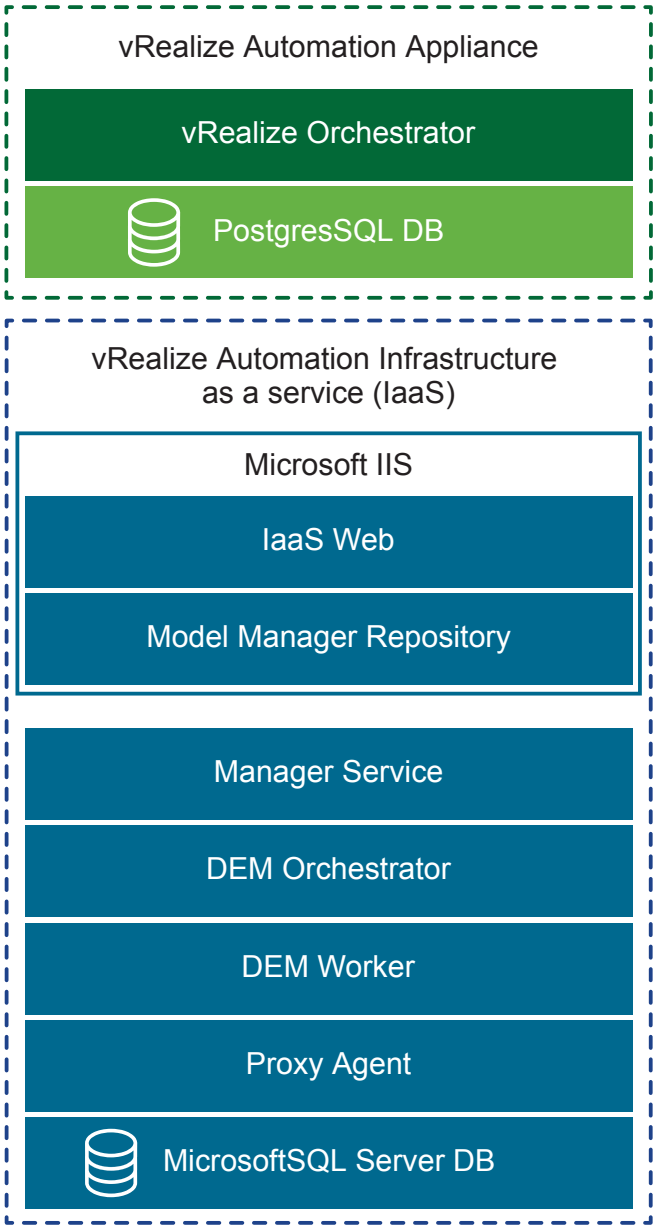
You can migrate to a minimal environment or to a high-availability environment.

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 6-1. vRealize Automation Minimal Deployment



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 **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 finish the 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 181 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

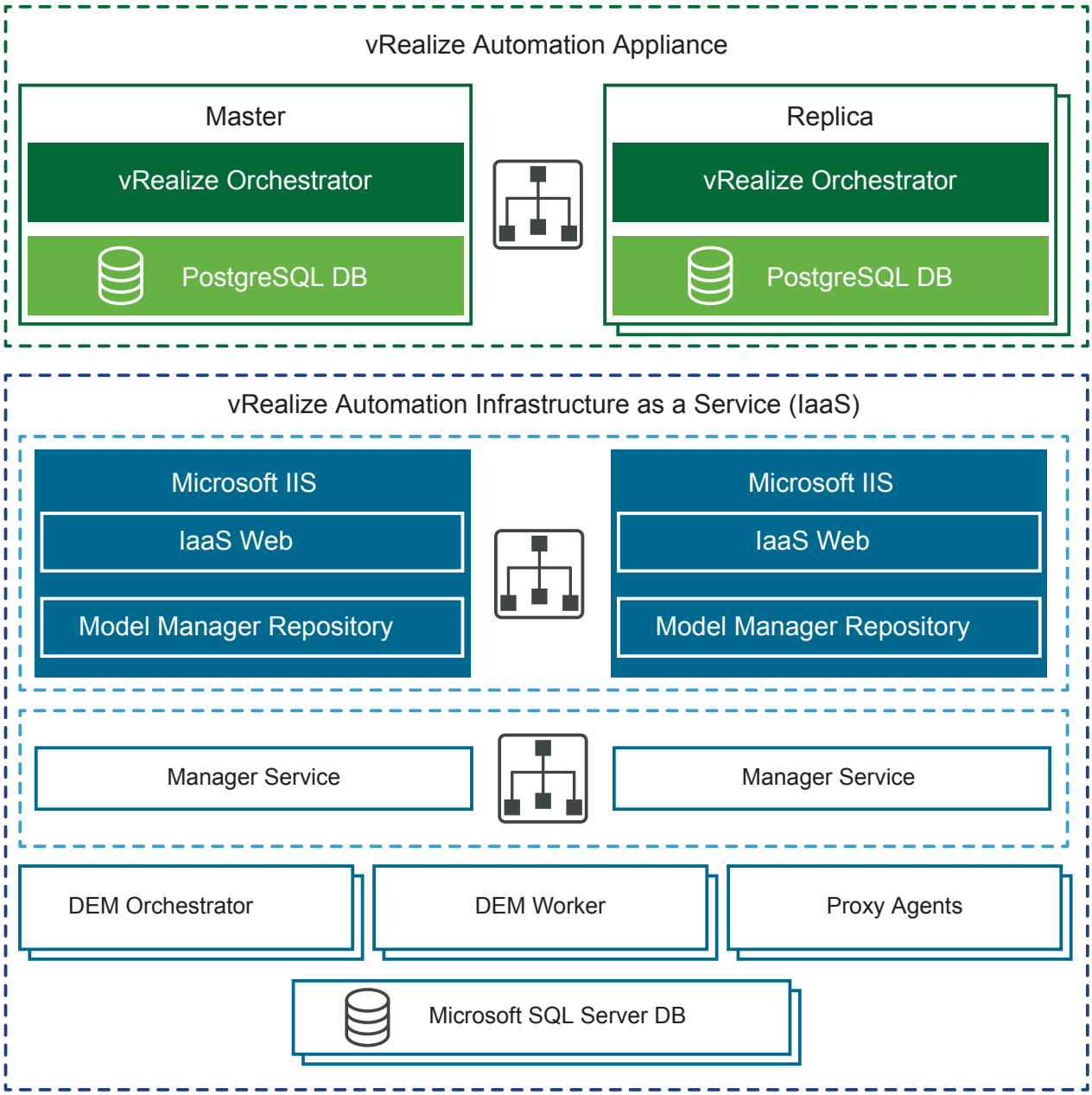
Pre-Migration Tasks.

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 6-2. vRealize Automation High-Availability Environment



Prerequisites

- Verify that you have a new target installation of vRealize Automation with a master and replica virtual appliances configured for high availability. See *vRealize Automation High Availability Configuration Considerations* in *Reference Architecture*.
- 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.
  a In your target vRealize Automation environment, log in to the vRealize Automation appliance management interface as root.

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

  b Select **Cluster**.

  c 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 finish 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 181 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 vRealize Automation Migration

vRealize Automation 7.1 and later introduces various functional changes during and after the upgrade process. If you are upgrading from a vRealize Automation 6.2.5 environment, review these changes before you begin your upgrade process.

For information about the differences between vRealize Automation 6.2.5 and 7.1 and greater, see *Review Changes Introduced by Migration from vRealize Automation 6.2.x* in *Migrating vRealize Automation*.

Note The vRealize Production Test Upgrade Assist Tool analyzes your vRealize Automation 6.2.5 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 6.2.5 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 7.1 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. 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.x or 7.3.x, 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.x or 7.3.x. Each version has its own hot fix.

Prerequisites

A running vRealize Automation 7.1.x or 7.3.x source vRealize Automation environment.

Procedure

- Apply this hot fix to your source vRealize Automation 7.1.x or 7.3.x appliance before you start migration. 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.

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 primary vRealize Automation appliance over SSH as **root**.

   If your vRealize Orchestrator is external, log in to the Orchestrator host machine.
2. Change directories to the PostgreSQL data folder on the primary host at `/var/vmware/vpostgres/current/pgdata/`.
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.

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 6-8. Source vRealize Automation Appliance

Option	Description	Value
Host name	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).	
Root username	root	
Root password	The root password that you entered when you deployed your source vRealize Automation appliance.	
Migration package location	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`.	

Table 6-9. Target vRealize Automation Appliance

Option	Description	Value
Root username	root	
Root password	The root password that you entered when you deployed your target vRealize Automation appliance.	
Default tenant	vsphere.local	
Administrator username	administrator	
Administrator password	Password for the administrator@vsphere.local user that you entered when you deployed the target vRealize Automation environment.	

Table 6-10. Target IaaS Database

Option	Description	Value
Database server	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.	
Cloned database name	Name of the source vRealize Automation6.2.x/7.x IaaS Microsoft SQL database cloned for migration.	

Table 6-10. Target IaaS Database (Continued)

Option	Description	Value
Authentication mode	Select either Windows or SQL Server. If you select SQL Server, you must enter a login name and password.	
Login name	Login name for the SQL Server user who has the db_owner role for the cloned IaaS Microsoft SQL database.	
Password	Password for the SQL Server user.	
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.	

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/BlnCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.
```

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

Option	Sample Input
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

Option	Sample Input
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.

Option	Sample Input
Domain Admin Password	Enter the password for the domain admin.
Bind User UPN	Use the email address format to enter the name of the user who can authenticate with the domain.
Bind DN Password	Enter the Active Directory bind account password for the account that can search for users.

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

Option	Sample Input
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

Option	Sample Input
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.
Bind User UPN	Use the email address format to enter the name of the user who can authenticate with the domain.
Bind DN Password	Enter the Active Directory bind account password for the account that can search for users.

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.

9 Select **Administration > Directories Management > Identity Providers**, and click your new identity provider.

   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 after you migrate from 7.1.x or later.

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 vRealize Automation. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation* in the PDFs section of vRealize Automation product documentation.

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 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 Minimal Environment.
- Migrate vRealize Automation Source Data to a vRealize Automation 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 Minimal Environment

You can migrate your current vRealize Automation environment data to a new release of vRealize Automation.

All tenants in the source system must be recreated in the target and go through the Migrate Identity Stores procedure.

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 **Migrate**.

2 Enter the information for the source vRealize Automation appliance.

Option	Description
Host name	The host name for the source vRealize Automation appliance.
Root username	`root`
Root password	The root password that you entered when you deployed the vRealize Automation appliance.
Migration package location	Path to an existing directory on the source vRealize Automation appliance where the migration package is created.

3 Enter the information for the target vRealize Automation appliance.

Option	Description
Root username	`root`
Root password	The root password that you entered when you deployed the target vRealize Automation appliance.
Default tenant	vsphere.local You cannot modify this field.
Administrator username	administrator You cannot modify this field.
Administrator password	Password for the administrator@vsphere.local user that you entered when you deployed the target vRealize Automation environment.

4 Enter the information for the target IaaS database server.

Option	Description
Database server	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.
Cloned database name	Name of the source vRealize Automation IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.
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 High-Availability Environment

You can migrate your current vRealize Automation environment data to a new release of vRealize Automation 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.

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 **Migrate**.
2. Enter the information for the source vRealize Automation appliance.

Option	Description
Host name	The host name for the source vRealize Automation appliance.
Root username	`root`
Root password	The root password that you entered when you deployed the source vRealize Automation appliance.

3. Enter the information for the migration package location on the source vRealize Automation appliance.

Option	Description
Migration package location	Path to an existing directory on the source vRealize Automation appliance where the migration package is created.

4 Enter the information for the target vRealize Automation appliance.

Option	Description
Root username	`root`
Root password	The root password that you entered when you deployed the target vRealize Automation appliance.
Default tenant	vsphere.local
Administrator username	administrator
Administrator password	Password for the administrator@vsphere.local user that you entered when you deployed the target vRealize Automation environment.

5 Enter the information for the target IaaS database server.

Option	Description
Database server	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.
Cloned database name	Name of the source vRealize Automation IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.
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.

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 vRealize Automation makes changes to endpoints in the target vRealize Automation environment.

After you migrate vRealize Automation, 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* in *Configuring vRealize Automation*.

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 Environment

After you migrate, you must run NSX Network and Security Inventory data collection in the target vRealize Automation environment.

This data collection is necessary for the Load Balancer Reconfigure action to work in the target vRealize Automation environment after migration.

Note You do not need to perform this data collection if you migrated from vRealize Automation 6.2.x.

Prerequisites

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.
- Successfully migrate to target vRealize Automation environment

.

Procedure

- Run NSX Network and Security Inventory data collection in your target vRealize Automation environment before you migrate to vRealize Automation. 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 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 7.5

You can migrate your existing external vRealize Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation.

Starting with vRealize Orchestrator 7.5, you can no longer upgrade your vRealize Orchestrator environments. To move vRealize Orchestrator environments to the latest version, you must migrate them.

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 vRealize Orchestrator server that is built into vRealize Automation. The migration from an external to embedded vRealize 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.

vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 6.0.3 Virtual Appliance	vRealize Automation 6.2.3	Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4
vRealize Orchestrator 6.0.4 on Windows	vRealize Automation 6.2.4	Migrate an External vRealize Orchestrator 6.x on Windows to vRealize Automation 7.4
vRealize Orchestrator 6.0.4 Virtual Appliance	vRealize Automation 6.2.4	Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4

vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 6.0.5 Virtual Appliance	vRealize Automation 6.2.5	Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4
vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c	vRealize Automation 7.0 or IaaS	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database	vRealize Automation 7.0.1 or IaaS	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.1 Virtual Appliance	vRealize Automation 7.1	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.2 Virtual Appliance	vRealize Automation 7.2	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2
vRealize Orchestrator 7.3 Virtual Appliance	vRealize Automation 7.3	Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4
vRealize Orchestrator 6.0.3 on Windows	vRealize Automation 6.2.3	Migrate the Orchestrator Configuration from Windows to Virtual Appliance

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* in *Installing and Configuring VMware vRealize Orchestrator*.
- 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 database of the source Orchestrator server, including the database schema.

  Note If you plan to use the source Orchestrator environment until the new one is fully configured, create a copy of the source database. Otherwise, you can configure the target Orchestrator to use the same database but in that case the source Orchestrator environment will no longer work because the database schema is upgraded to the version of the target Orchestrator.

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
```

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
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

The default database login information is:

database_name	vmware
database_user	vmware
database_user_password	vmware

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 Embedded vRealize Orchestrator Server Service.

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.

```
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.

```
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.

```
./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
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

The default database login information is:

database_name	vmware
database_user	vmware
database_user_password	vmware

6 Remove all certificates from the database keystore.

```
./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 Embedded vRealize Orchestrator Server Service.

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.

```
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.

```
./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
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

The default database login information is:

database_name	vmware
database_user	vmware
database_user_password	vmware

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 Embedded vRealize Orchestrator Server Service.

Configure the Embedded vRealize Orchestrator Server Service

After you migrate an external vRealize Orchestrator configuration and import it to vRealize Automation, you configure the vRealize Orchestrator server service.

Procedure

1 In the vRealize Automation appliance management interface, under **Services**, verify that the embedded `vco` service is REGISTERED.

2 Select the `vco` service of the external vRealize Orchestrator server that you have migrated 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* in *Installing and Configuring VMware vRealize Orchestrator*.
- 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.

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.

Menu Item	Details
Licensing	The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.
Export/Import Configuration	The embedded Orchestrator configuration is included in the exported vRealize Automation components.

Menu Item	Details
Configure Database	The embedded Orchestrator uses the database that is used by vRealize Automation.
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.

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.

If you find endpoints containing the FQDN, complete these steps.	If you do not find endpoints containing the FQDN, complete these steps.
1 Click **Workflows**. 2 Click the expand button to select **Library > vRealize Automation > Configuration**. 3 Do one of these steps. ■ 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.	1 Click **Resources**. 2 Click the update icon on the top toolbar. 3 Click the expand button to select **Library > vCACCAFE > Configuration**. 4 Do one of these steps. ■ 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.

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.

If you find endpoints containing the FQDN, complete these steps.	If you do not find endpoints containing the FQDN, complete these steps.
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* in *Life Cycle Extensibility*.

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 6.2.5 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 to the target vRealize Automation release.
- 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.

Reconfigure the Microsoft Azure Endpoint in the Target vRealize Automation Environment

After migration, you must reconfigure your Microsoft Azure endpoint.

Perform this procedure for each Microsoft Azure endpoint.

Prerequisites

- Successfully migrate to the target 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 as a IaaS administrator user.

Procedure

1 Select **Administration > vRO Configuration > Endpoints**.

2 Select a Microsoft Azure endpoint.

3 Click **Edit**.

4 Click **Details**.

5 Select the region in the Azure environment drop-down menu.

6 Enter the original client secret in the client secret text box.

7 Enter the storage URL in the Azure storage URI text box.

Example: https://mystorageaccount.blob.core.windows.net

8 Click **Finish**.

9 Repeat for each Azure endpoint.

Migrate vRealize Automation 6.2.x Automation Application Services

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 the target vRealize Automation version.

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* in *Configuring vRealize Automation*.

Upgrading Software Agents to TLS 1.2

After you migrate vRealize Automation, 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 source environment as well as any existing virtual machines.

Update Source Environment Virtual Machine Templates

You must update existing, migrated vRealize Automation templates after you complete migration 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 migrated vRealize Automation template 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

- Successful migration from vRealize Automation 7.1x or later.
- Apply Software Agent Patch if you migrated from vRealize Automation 7.1.xor 7.3.x.

Procedure

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 **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

- Migrate vRealize Automation 7.1.x or later.
- Apply Software Agent Patch if you migrated from vRealize Automation 7.1.x or 7.3.x.
- Log in to the target vRealize Automation environment on the primary virtual appliance.

Procedure

1. Click **Administration > Health**.
2. Click **New Configuration**.
3. On the Configuration Details page, provide the requested information.

Option	Comment
Name	Enter `SW Agent verification`
Description	Add optional description, for example, `Locate software agents for upgrade to TLS 1.2`
Product	Select the target product and version, for example vRealize Automation 7.4.0.
Schedule	Select None.

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 6-11. vRealize Automation Virtual Appliance

Option	Description
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 6-12. vRealize Automation System Tenant

Option	Description
System Tenant Administrator	administrator
System Tenant Password	Password for administrator.

Table 6-13. vRealize Automation Disk Space Monitoring

Option	Description
Warning Threshold Percent	Accept default: 75
Critical Threshold Percent	Accept default: 90

Table 6-14. vRealize Automation Tenant

Option	Description
Tenant Under Test	Tenant selected for testing.
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 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 the target vRealize Automation release.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1.x or 7.3.x.
- Successful migration from vRealize Automation 7.1.x or later.
- 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 > 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.

Option	Description
Tenant name	Name of tenant on the source vRealize Automation appliance. **Note** The tenant user must have the Software Architect role assigned.
Username	Tenant administrator user name on the source vRealize Automation appliance.
Password	Tenant administrator password.

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.

Option	Description
Batch Size	The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.
Queue Depth	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.
Batch Errors	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.
Batch Failures	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.
Batch Polling	How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.

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 Microsoft Azure

You can upgrade outdated software agents on Amazon Web Service (AWS) or Microsoft Azure manually.

- You must update the tunnel properties specified in the reservation of the migrated vRealize Automation server.

Note Replace any version instances in these examples with the vRealize Automation version value of your target release.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1.x or 7.3.x.
- Successful migration from vRealize Automation 7.1.x or later.
- 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 Amazon AWS or Microsoft Azure endpoint.

```
"key": "ipAddress",

        "value": {

            "type": "string",

            "value": "<$PrivateIp:$PrivatePort>"

        }
```

- Use this command for updating a Linux machine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py –a <$DestionationVRAServer>
–t <$Tenant> –S <$SourceVRAServer> –tu <$TenantUser> –CL Software.LinuxAgentUpdate74 ––
source_cloud_provider azure
```

- Use this command for updating a Windows machine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py –a <$DestionationVRAServer>
–t <$Tenant> –S <$SourceVRAServer> –tu <$TenantUser> –CW Software.WindowsAgentUpdate74 ––
source_cloud_provider azure
```

- This command runs the plan file.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py –a <$DestionationVRAServer>
–t <$Tenant> –tu <$TenantUser> ––plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

3 Use this command to update the software agent using the node file from step 1 and the plan file from step 2.

```
/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 plan_batch –S <$SourceVRAServer>
```

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 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 `Text Box` (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 `Text Box` (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 `TestOverideLabel` 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
TestOverideLabel:
  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 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 6-15. Source vRealize Automation Appliance

Log	Location
Package creation log	`/var/log/vmware/vcac/migration-package.log`

Table 6-16. Target vRealize Automation Appliance

Log	Location
Migration log	`/var/log/vmware/vcac/migrate.log`
Migration execution log	`/var/log/vmware/vcac/mseq.migration.log`
Migration execution output log	`/var/log/vmware/vcac/mseq.migration.out.log`
Validation execution log	`/var/log/vmware/vcac/mseq.validation.log`
Validation execution output log	`/var/log/vmware/vcac/mseq.validation.out.log`

Table 6-17. Target vRealize Automation Infrastructure Nodes

Log	Location
Migration log	`C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log`
Validation log	`C:\Program Files (x86)\VMware\vCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log`

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.
   a. Select **Administration > Property Dictionary > Property Definitions**.
   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.

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 s string such as "ping" reported back for *version*.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 version value in the target virtual appliance.
- Between these events, observe the updateSoftwareAgents.log file at /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log

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 fluctuate during the upgrade process:

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-
a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error
while polling events for subscription '{}'

org.springframework.web.client.HttpClientErrorException: 404 Not Found

org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultRespon
seErrorHandler.java:91) ~[nobel-agent.jar:na]

org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641)
~[nobel-agent.jar:na]

org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597)
~[nobel-agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]
```

Enable Your Load Balancers

7

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 vRealize Automation Documentation .

Change the load balancer timeout settings from 10 minutes back to the default.

Post-Upgrade Tasks for Upgrading vRealize Automation 8

After you upgrade from vRealize Automation 7.1, 7.2, or 7.3.x to 7.4, you must perform required post-upgrade tasks.

This chapter includes the following topics:

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.

Option	Comment
Name	Enter `SW Agent verification`.
Description	Add optional description, for example, `Locate software agents for upgrade to TLS 1.2`.
Product	Select vRealize Automation 7.4.0.
Schedule	Select **None**.

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 8-1. vRealize Automation Virtual Appliance

Option	Description
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 8-2. vRealize Automation System Tenant

Option	Description
System Tenant Administrator	administrator
System Tenant Password	Password for administrator.

Table 8-3. vRealize Automation Disk Space Monitoring

Option	Description
Warning Threshold Percent	Accept default: 75
Critical Threshold Percent	Accept default: 90

Table 8-4. vRealize Automation Tenant

Option	Description
Tenant Under Test	Tenant selected for testing.
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.

Option	Description
Tenant name	Name of tenant on the upgraded vRealize Automation appliance. **Note** The tenant user must have the Software Architect role assigned.
Username	Tenant administrator user name on the vRealize Automation appliance.
Password	Tenant administrator password.

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.

Option	Description
Batch Size	The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.
Queue Depth	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.
Batch Errors	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.

Option	Description
Batch Failures	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.
Batch Polling	How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.

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.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestionationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Use this command for updating a Windows machine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestionationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- This command runs the plan file.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestionationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

3 Use this command to update the Software Agent using the node file from step 1 and the plan file from step 2.

```
/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 plan_batch -S <$SourceVRAServer>
```

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* in *Configuring vRealize Automation*.

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 your source vRealize Automation environment before you migrate to vRealize Automation 7.4. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation*.

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.

2 Change directories to `/usr/lib/vcac/tools/vami/commands`.

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

9

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.

This chapter includes the following topics:

- Work Around Upgrade Problems
- Virtual Appliance Upgrade Fails During the IaaS Prerequisite Check

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.
  a Log in to the master vRealize Automation appliance node as **root** using SSH.
  b Run `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`.
  c 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.
  a Open a command prompt on a Manager Service node.

b Navigate to the vRealize Automation installation folder and open the Manager Service configuration file at `VMware\vCAC\Server\ManagerService.exe.config`.

c 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.

  a Log in to the master vRealize Automation appliance node as **root** using SSH.

  b Run `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE`.

  c 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.

  a Open a command prompt on a Manager Service node.

  b Navigate to the vRealize Automation installation folder and open the Manager Service configuration file at `VMware\vCAC\Server\ManagerService.exe.config`.

  c 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 NodeId: *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. --->

  System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: 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.
- Warning: Non-zero return code. Command failed.

- 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 DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
  at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2 decryptFunc)
  at DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object sender, ObjectMaterializedEventArgs e)
  at System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
  at System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
  at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
  at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
  at DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(CoreModelEntities coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
  at DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
  at DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String

coreModelConnectionString)

at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

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:

```
<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\xmldb\ 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:

   ```
   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/VSPHERE.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 user name **`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.
  a Open a browser and navigate to the vRealize Automation IaaS installation page on thevRealize 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.

Parameter	Short Name	Description
--DatabaseSyncTimeout	-dstm	Sets the http request timeout value only for `SynchronizeDatabases` in seconds.
--DatabaseSyncPageSize	-dsps	Sets the sync request page size only for Reservation or Reservation Policy synchronization. The default is 10.

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 9-1. Available Flags

Flag	Description
/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.

Table 9-1. Available Flags (Continued)

Flag	Description
/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 Mfrontanager data, and Manager Service. **Note** This flag also prevents enabling the Manager Service automatic failover mode.
/tmp/do-not-upgrade-dems	Prevents DEM upgrade.
/tmp/do-not-upgrade-agents	Prevents IaaS proxy agent upgrade.

3 Complete the tasks for your chosen flag.

Table 9-2. Additional Tasks

Flag	Tasks
/tmp/disable-iaas-upgrade	■ Upgrade the Management Agent manually. ■ Apply any required IaaS prerequisites manually. ■ 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. a Each VMware vRealize Automation Proxy Agent. b Each VMware DEM worker. c The VMware DEM orchestrator. d The VMware vCloud Automation Center service. ■ Start the IaaS upgrade manually after the virtual appliance upgrade is complete.
/tmp/do-not-upgrade-ma	Upgrade the Management Agent manually.
/tmp/skip-prereq-checks	Apply any required IaaS prerequisites manually.

Table 9-2. Additional Tasks (Continued)

Flag	Tasks
/tmp/do-not-stop-services	Manually stop the IaaS services. 1 Log in to your IaaS Windows server. 2 Select **Start > Administrative Tools > Services**. 3 Stop these services in the following order. **Note** Do not shut down the IaaS Windows server. a Each VMware vRealize Automation Proxy Agent. b Each VMware DEM worker. c The VMware DEM orchestrator. d The VMware vCloud Automation Center service.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

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 the vRealize Automation Appliance.