Migrating vRealize Automation to 7.4

03 May 2018
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

This *Migrating vRealize Automation to 7.4* is updated with each release of the product or when necessary.

This table provides the update history of *Migrating vRealize Automation to 7.4*.

Revision	Description
03 MAY 2018	Added section containing guidance for Migrating an External Orchestrator Server to vRealize Automation 7.4.
12 APR 2018	Initial release.

1 Migrating vRealize Automation

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

Migration moves all data, except for tenants and identity stores, from your current vRealize Automation source environment to a target deployment of the latest version of vRealize Automation. In addition, migration moves all data from the embedded vRealize Orchestrator 7.x to the target deployment.

Migration does not change your source environment except to stop vRealize Automation services for the time required to collect and copy the data safely to your target environment. Depending on the size of the source vRealize Automation database, migration can take from a few minutes to hours.

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

If you plan to put your target environment into production after migration, do not put your source environment back into service. Changes to your source environment after migration are not synchronized with your target environment.

If your source environment is integrated with vCloud Air or vCloud Director or has physical endpoints, you must use migration to perform an upgrade. Migration removes these endpoints and everything associated with them from the target environment. Migration also removes a 6.x
VMware vRealize Application Services integration from the target environment.

Note You must complete additional tasks to prepare your vRealize Automation virtual machines before you migrate. Before you migrate, review Knowledge Base article 51531.

If you migrate from vRealize Automation 6.2.x to the latest version, you might experience these issues.

Issue	Resolution
After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request. ■ Control types: Check box or link. ■ Attributes: Relationship, regular expressions, or property layouts. In vRealize Automation 7.x, the property definitions no longer use these elements.	You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request.
Regular expressions used to define the parent-child relationships in a vRealize Automation 6.2.x drop-down menu are not supported in 7.x. In 6.2.x, you can use regular expressions to define one or more child menu items that are only available for a certain parent menu item. Only those child menu items appear when you select the parent menu item. After migration to 7.x , all the available menu items appear in the child drop-down menu regardless of what you choose in the parent drop-down menu. To show that previously defined dynamic values no longer work, the first menu item in the child drop-down menu reads "Warning! Use vRO workflows to define dynamic values."	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

2

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 2-1. vRealize Automation 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 2-2. vRealize Automation

Purpose	Access	Required Credentials
You use vRealize Automation for these tasks. ■ Request new IT services. ■ 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 2-3. 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 2-4. 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 2-5. 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 2-6. 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 2-7. 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

3

The migration prerequisites differ depending on your target environment.

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

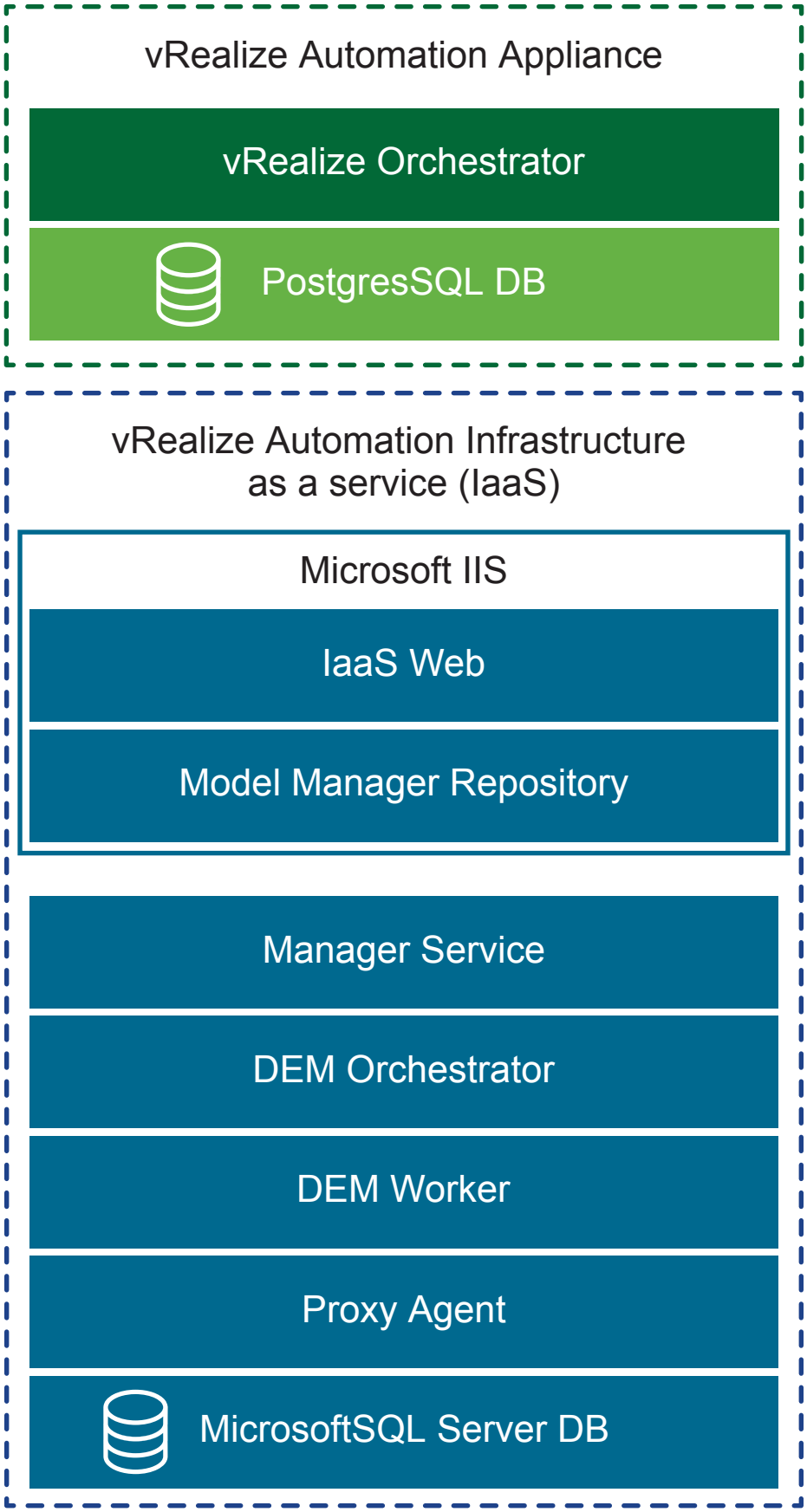
This chapter includes the following topics:

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 3-1. 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 **vRA Settings > Cluster**.

  c Expand the Host / Node Name records by clicking the triangle.

  Verify that the version numbers of the vRealize Automation IaaS components match.
- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.
- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.
- Verify that the endpoint vCenter has sufficient resources to complete migration.
- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.
- Verify that the IaaS server node in the target environment has at least Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. After you install the JRE, make sure the JAVA_HOME environment variable points to the Java version you installed on each IaaS node. Revise the path if necessary.
- Verify that each IaaS node has PowerShell 3.0 or later installed.

- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.

What to do next

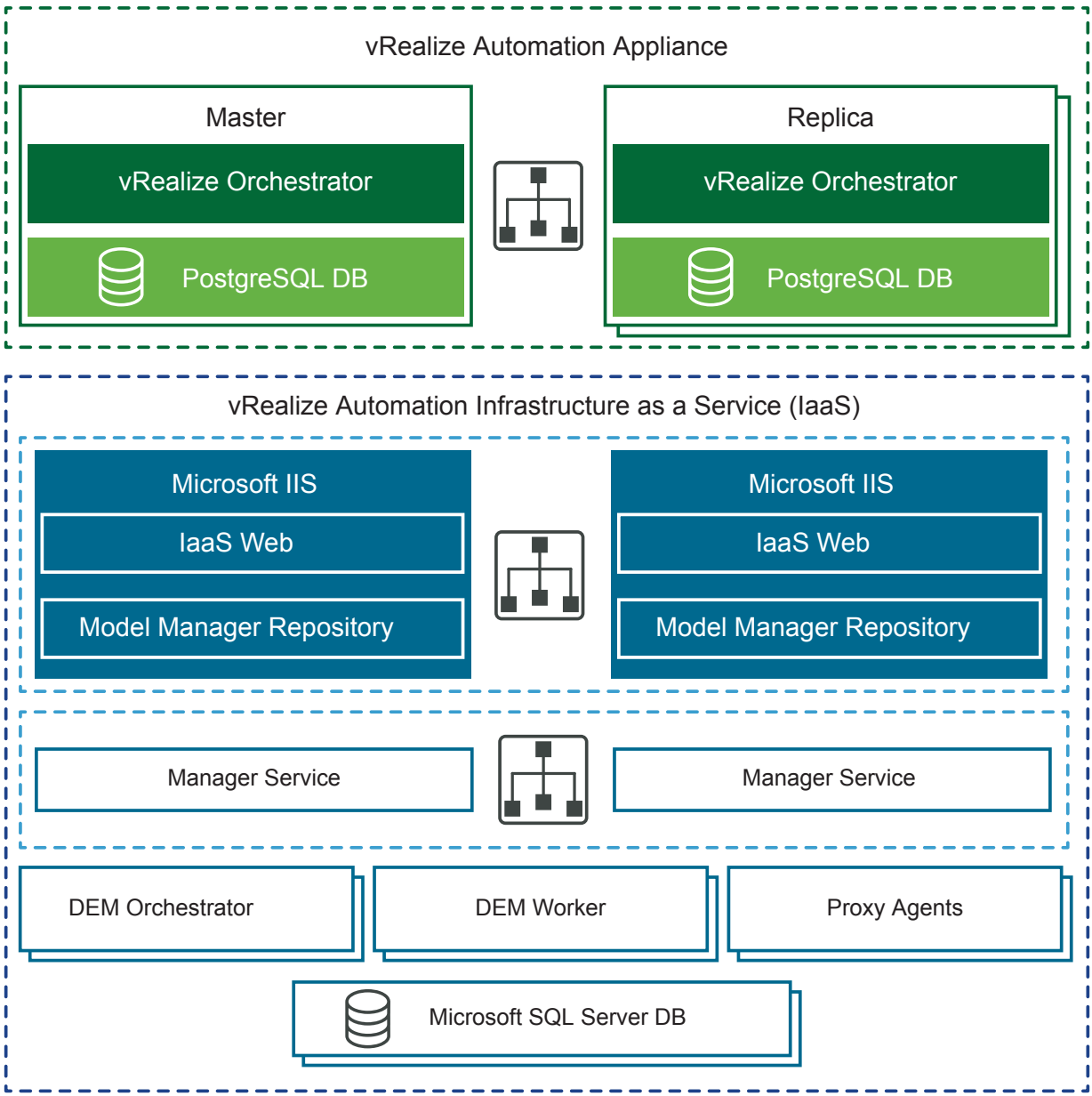
Chapter 4 Pre-Migration Tasks.

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 3-2. 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, start a browser and go to the vRealize Automation appliance management console at `https:// vra-va-hostname.domain.name:5480`.

  b Log in with the user name root and the password you entered when you deployed the appliance.

  c Select **vRA Settings > Cluster**.

  d To expand the Host / Node Name records so you can see the components, click the expand button.

  Verify that the version numbers of vRealize Automation components match across all virtual appliance nodes.

  Verify that the version numbers of vRealize Automation IaaS components match across all IaaS nodes.
- Review Knowledge Base article 51531.
- Perform these steps to direct traffic to only the master node.
  a Disable all the redundant nodes.

b Remove the health monitors for these items according to your load balancer documentation:

- vRealize Automation virtual appliance
- IaaS Website
- IaaS Manager Service

- Verify that the target Microsoft SQL Server version for the vRealize Automation target IaaS database is 2012, 2014, or 2016.
- Verify that port 22 is open between the source and target vRealize Automation environments. Port 22 is required to establish Secure Shell (SSH) connections between source and target virtual appliances.
- Verify that the endpoint vCenter has sufficient resources to complete migration.
- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.
- Verify that the target vRealize Automation environment system time is synchronized between Cafe and the IaaS components.
- Verify that the IaaS Web Service and Model Manager nodes in the target environment have the right Java Runtime Environment. You must have Java SE Runtime Environment (JRE) 8, 64 bit, update 161 or later installed. Make sure the JAVA_HOME system variable points to the Java version you installed on each IaaS node. Revise the path if necessary.
- Verify that each IaaS node has at least PowerShell 3.0 or later installed.
- Verify that the source and target vRealize Automation environments are running.
- Verify that no user and provisioning activities are happening on the source vRealize Automation environment.
- Verify that any antivirus or security software running on IaaS nodes in the target vRealize Automation environment that might interact with the operating system and its components is correctly configured or disabled.

What to do next

Chapter 4 Pre-Migration Tasks.

Pre-Migration Tasks

4

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.

This chapter includes the following topics:

Review Changes Introduced by Migration from vRealize Automation 6.2.x to 7.x

vRealize Automation 7 and later introduces various functional changes during and after the upgrade process. Review these changes before you upgrade your vRealize Automation 6.2.x deployment to the latest version.

For information about the differences between vRealize Automation 6.2.x and 7.x, see Considerations About Upgrading to This vRealize Automation Version in *Upgrading vRealize Automation 6.2.5 to 7.4*.

Note The vRealize Production Test Upgrade Assist Tool analyzes your vRealize Automation 6.2.x environment for any feature configuration that can cause upgrade issues and checks that your environment is ready for upgrade. To download this tool and related documentation, go to the VMware vRealize Production Test Tool download product page.

After you migrate from vRealize Automation 6.2.x to the latest version, catalog items that use these property definitions appear in the service catalog but are not available to request.

- Control types: Check box or link.
- Attributes: Relationship, regular expressions, or property layouts.

In vRealize Automation 7.x, the property definitions no longer use these elements. You must recreate the property definition or configure the property definition to use a vRealize Orchestrator script action rather than the embedded control types or attributes. For more information, see Catalog Items Appear in the Service Catalog After Migration But Are Not Available to Request.

Apply Software Agent Patch

Before you migrate from vRealize Automation 7.1 or 7.3 to 7.4, you must apply a hot fix to the source appliance so that you can upgrade Software Agents to TLS 1.2.

The Transport Layer Security (TLS) protocol provides data integrity between your browser and vRealize Automation. This hot fix makes it possible for the Software Agents in your source environment to upgrade to TLS 1.2. This upgrade ensures the highest level of security and is required for vRealize Automation 7.1 or 7.3. Each version has its own hot fix.

Prerequisites

A running vRealize Automation 7.1 or 7.3 source environment.

Procedure

- Apply this hot fix to your source vRealize Automation 7.1 or 7.3 appliance before you migrate to 7.4. See Knowledge Base article 52897.

What to do next

Change DoDeletes Setting on the vSphere Agent to False.

Change DoDeletes Setting on the vSphere Agent to False

If you migrate from a vRealize Automation 6.2.4 environment, you must change the DoDeletes setting on your target vSphere agent before migration. This prevents virtual machines from your source environment being deleted after migration.

Follow the steps in the Configure the vSphere Agent procedure in *Installing vRealize Automation* to set DoDeletes to false.

Prerequisites

You have completed the prerequisites for migration.

What to do next

Prepare vRealize Automation Virtual Machines for Migration.

Check Templates in Your vRealize Automation 6.x Source Environment

Before you migrate from a vRealize Automation 6.x to 7.4, 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 6.x source environment with less than 4 MB of memory, migration fails. Complete this procedure to determine if any blueprints in the 6.x source environment have less than 4 MB of memory.

Prerequisites

You are migrating from vRealize Automation 6.x to 7.4.

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 4-1. 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	

Table 4-1. Source vRealize Automation Appliance (Continued)

Option	Description	Value
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 4-2. 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 4-3. 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.	
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.Encryption
KeyTool.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.

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.
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**.

Option	Sample Input
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 7.4 when you migrate from 7.1, 7.2, or 7.3 deployments.

Note You do not need to run this data collection in your source environment when you migrate from vRealize Automation 6.2.x. vRealize Automation 6.2.x does not support the Load Balancer Reconfigure action.

Procedure

- Run NSX Network and Security Inventory data collection in your source vRealize Automation environment before you migrate to vRealize Automation 7.4. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation*.

What to do next

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database

Before migration, you must back up your IaaS Microsoft SQL database in the vRealize Automation source environment and restore it to a new blank database created in the vRealize Automation target environment.

Prerequisites

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment.

- Obtain information about backing up and restoring an SQL Server database. Find articles on the Microsoft Developer Network about creating a full SQL Server database backup and restoring an SQL Server database to a new location.

Procedure

- Create a full backup of your source vRealize Automation 6.2.x or 7.x IaaS Microsoft SQL database. You use the backup to restore the SQL database to a new blank database created in the target environment.

What to do next

Snapshot the Target vRealize Automation Environment.

Snapshot the Target vRealize Automation Environment

Take a snapshot of each target vRealize Automation virtual machine. If migration is unsuccessful, you can try again using the virtual machine snapshots.

For information, see your vSphere documentation.

Prerequisites

Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.

What to do next

Perform one of the following procedures:

- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment.
- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

Migration Procedures

5

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.

This chapter includes the following topics:

- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment
- Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 Minimal Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4.

Prerequisites

- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a Minimal Environment.
- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as **root** using the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1 Select **vRA Settings > Migration**.

2 Enter the information for the source vRealize Automation appliance.

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 6.2.x or 7.x 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 6.2.x or 7.x 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.

Option	Description
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

Chapter 6 Post-Migration Tasks.

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment

You can migrate your current vRealize Automation environment data to a new installation of vRealize Automation 7.4 configured as a high-availability environment.

Prerequisites

- Gather Information Required for Migration.
- Obtain the Encryption Key from the Source vRealize Automation Environment.
- Add Each Tenant from the Source vRealize Automation Environment to the Target Environment.
- Create an Administrator for Each Added Tenant.
- Synchronize Users and Groups for an Active Directory Link Before Migration to a High-Availability Environment.

- Manually Clone the Source vRealize Automation IaaS Microsoft SQL Database.
- Snapshot the Target vRealize Automation Environment.
- Log in to the target vRealize Automation Appliance Management as **root** using the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1. Select **vRA Settings > Migration**.
2. Enter the information for the source vRealize Automation appliance.

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 6.2.x or 7.x 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 6.2.x or 7.x IaaS Microsoft SQL database that you backed up on the source and restored on the target environment.

Option	Description
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

Chapter 6 Post-Migration Tasks.

Post-Migration Tasks

6

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.

This chapter includes the following topics:

Add Tenant and IaaS Administrators from the Source vRealize Automation 6.2.x Environment

You must delete and restore the vRealize Automation 6.2.x tenant administrators in each tenant after migration.

Perform the following procedure for each tenant in the target vRealize Automation console.

Note If you migrate from a vRealize Automation 7.x environment, you do not need to perform this procedure.

Prerequisites

- Successful migration to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console as **Administrator** with the password you entered when you deployed the target vRealize Automation appliance.

Procedure

1. Select **Administration > Tenants**.
2. Click a tenant name.
3. Click **Administrators**.
4. Make a list of each tenant administrator name and user name.
5. Point to each administrator and click the delete icon (Delete) until you delete all administrators.
6. Click **Finish**.
7. On the Tenants page, click the tenant name again.
8. Click **Administrators**.
9. Enter the name of each user that you deleted in the appropriate search box and press Enter.
10. Click the name of the appropriate user from the search returns to add the user back as an administrator.

    When you finish, the list of tenant administrators looks the same as the list of administrators you deleted.
11. Click **Finish**.

Run Test Connection and Verify Migrated Endpoints

Migrating to vRealize Automation 7.4 makes changes to endpoints in the target environment.

After you migrate to vRealize Automation 7.4, you must use the **Test Connection** action for all applicable endpoints. You might also need to make adjustments to some migrated endpoints. For more information, see *Considerations When Working With Upgraded or Migrated Endpoints* 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 7.4 Environment

After you migrate, you must run NSX Network and Security Inventory data collection in the target vRealize Automation 7.4 environment.

This data collection is necessary for the Load Balancer Reconfigure action to work in vRealize Automation 7.4 for 7.1, 7.2, and 7.3 deployments.

Note You do not need to perform this data collection if you migrated from vRealize Automation 6.2.x to 7.4.

Prerequisites

- Run NSX Network and Security Inventory Data Collection in the Source vRealize Automation Environment .
- Successfully migrate to vRealize Automation 7.4.

Procedure

- Run NSX Network and Security Inventory data collection in your target vRealize Automation environment before you migrate to vRealize Automation 7.4. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation*.

Reconfigure Load Balancers After Migration to a High-Availability Environment

When you migrate to a high-availability environment, you must perform these tasks for each load balancer after you finish migration.

Prerequisites

Migrate vRealize Automation Source Data to a vRealize Automation 7.4 High-Availability Environment.

Procedure

1. Restore the original health check settings so replica nodes can accept incoming traffic by configuring the load balancers for these items.
   - vRealize Automation appliance.
   - IaaS Web Server that hosts the Model Manager.
   - Manager Service.
2. Change the load balancer timeout settings back to the default.

Migrating an External Orchestrator Server to vRealize Automation 7.4

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

You can deploy vRealize Orchestrator as an external server instance and configure vRealize Automation to work with that external instance, or you can configure and use the vRealize Orchestrator server that is included in the vRealize Automation appliance.

VMware recommends that you migrate your external vRealize Orchestrator to the Orchestrator server that is built into vRealize Automation. The migration from an external to embedded Orchestrator provides the following benefits:

- Reduces the total cost of ownership.
- Simplifies the deployment model.

- Improves the operational efficiency.

Note Consider using the external vRealize Orchestrator in the following cases:

- Multiple tenants in the vRealize Automation environment.
- Geographically dispersed environment.
- Workload handling.
- Use of specific plug-ins, such as the Site Recovery Manager plug-in versions earlier than 6.5.

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

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 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 Deployment	vRealize Automation Deployment	Migration Scenario
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 Built-In vRealize Orchestrator Server.

Migrate an External vRealize Orchestrator 6.x Virtual Appliance to vRealize Automation 7.4

After you upgrade your vRealize Automation from version 6.x to version 7.4, you can migrate your existing external Orchestrator 6.x Virtual Appliance to the Orchestrator server that is built into vRealize Automation 7.4.

Note If you have a distributed vRealize Automation environment with multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

Prerequisites

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see *Upgrading vRealize Automation* in *Installing or Upgrading vRealize Automation*.

- If the source Orchestrator uses a SHA1 package-signing certificate, make sure to regenerate the certificate using a stronger signing algorithm. The recommended signing algorithm is SHA2.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1. Download the migration tool from the target Orchestrator server to the source Orchestrator.
   a. Log in to the vRealize Orchestrator 6.x Virtual Appliance over SSH as **root**.
   b. Under the `/var/lib/vco` directory, run the `scp` command to download the `migration-tool.zip` archive.

      ```
      scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
      ```

   c. Run the `unzip` command to extract the migration tool archive.

      ```
      unzip migration-tool.zip
      ```

2. Export the Orchestrator configuration from the source Orchestrator server.
   a. In the `/var/lib/vco/migration-cli/bin` directory, run the `export` command.

      ```
      ./vro-migrate.sh export
      ```

      This command combines the VMware vRealize Orchestrator configuration files and plug-ins into an export archive.

      An archive with file name `orchestrator-config-export-`*`orchestrator_ip_address-date_hour`*`.zip` is created in the `/var/lib/vco` folder.

3. Migrate the exported configuration to the Orchestrator server that is built into vRealize Automation 7.4.
   a. Log in to the vRealize Automation appliance over SSH as **root**.
   b. Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

      ```
      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-configuration.sh untrust --reset-db
```

7 Reinstall the Orchestrator plug-ins.

a Log in to Control Center as **root**.

b Click **Troubleshooting**.

c Click **Force plug-ins reinstall**.

8 Start the Orchestrator server service.

9 Revert to the default configuration of the `postgresql.conf` and the `pg_hba.conf` file.

a Restart the PostgreSQL server service.

You successfully migrated an external vRealize Orchestrator 6.x Virtual Appliance to a vRealize Orchestrator instance embedded in vRealize Automation 7.4.

What to do next

Set up the built-in vRealize Orchestrator server. See Configure the Built-In vRealize Orchestrator Server.

Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.4

You can export the configuration from your existing external Orchestrator instance and import it to the Orchestrator server that is built into vRealize Automation.

Note If you have multiple vRealize Automation appliance nodes, perform the migration procedure only on the primary vRealize Automation node.

Prerequisites

- Upgrade or migrate your vRealize Automation to version 7.4. For more information, see *Upgrading vRealize Automation* in *Installing or Upgrading vRealize Automation*.
- Stop the Orchestrator server service of the external Orchestrator.
- Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1 Export the configuration from the external Orchestrator server.

   a Log in to Control Center of the external Orchestrator server as **root** or as an **administrator**, depending on the source version.

   b Stop the Orchestrator server service from the **Startup Options** page to prevent unwanted changes to the database.

   c Go to the **Export/Import Configuration** page.

   d On the **Export Configuration** page, select **Export server configuration**, **Bundle plug-ins** and **Export plug-in configurations**.

2 Migrate the exported configuration into the embedded Orchestrator instance.

   a Upload the exported Orchestrator configuration file to the `/usr/lib/vco/tools/configuration-cli/bin` directory of the vRealize Automation appliance.

   b Log in to the vRealize Automation appliance over SSH as **root**.

   c Stop the Orchestrator server service and the Control Center service of the built-in vRealize Orchestrator server.

```
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 an external vRealize Orchestrator configuration and import it to vRealize Automation, you configure the vRealize Orchestrator server that is built into vRealize Automation.

Prerequisites

Migrate the configuration from the external to the internal vRealize Orchestrator.

Procedure

1 Log in as root to a command prompt session on the vRealize Automation appliance.

2 Start services for the vRealize Orchestrator Control Center and server:

```
service vco-configurator start && service vco-server start
```

3 Log in as root to the built-in vRealize Orchestrator Control Center.

https://*vrealize-automation-appliance-FQDN*:8283/vco-controlcenter/config

Note You can skip the next step when the external and internal vRealize Orchestrator versions are the same.

4 In Control Center, click **Validate Configuration**, and verify that vRealize Orchestrator is configured properly.

5 In Control Center, click **Certificates**, click **Package Signing Certificate**, and generate a new package signing certificate.

6 In Control Center, click **Configure Authentication Provider**.

Default tenant and **Admin group** are set to default values `vsphere.local` and `vsphere.local\vcoadmins`. Change the defaults to the values for your environment.

7 In the vRealize Automation appliance management interface, under **Services**, verify that `vco-server` is REGISTERED.

8 Select the `vco` services of the external vRealize Orchestrator server, and click **Unregister**.

What to do next

- Import any certificates that were trusted in the external vRealize Orchestrator server to the trust store of the built-in vRealize Orchestrator. For more information, see *Manage Orchestrator Certificates* in *Installing and Configuring VMware vRealize Orchestrator*.
- Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the vRealize Orchestrator configuration.

  For more information, see *Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability* in *Installing or Upgrading vRealize Automation*.

  Note The vRealize Orchestrator instances are automatically clustered and available for use.

- Restart the `vco-configurator` service on all nodes in the cluster.
- Update the vRealize Orchestrator endpoint to point to the migrated built-in vRealize Orchestrator server.
- Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.

Update Embedded vRealize Orchestrator to Trust vRealize Automation Certificates

If you update or change vRealize Automation appliance or IaaS certificates, you must update vRealize Orchestrator to trust the new or updated certificates.

This procedure applies to all vRealize Automation deployments that use an embedded vRealize Orchestrator instance. If you use an external vRealize Orchestrator instance, see Update External vRealize Orchestrator to Trust vRealize Automation Certificates.

Note This procedure resets tenant and group authentication back to the default settings. If you have customized your authentication configuration, note your changes so that you can re-configure authentication after completing the procedure.

See the vRealize Orchestrator documentation for information about updating and replacing vRealize Orchestrator certificates.

If you replace or update vRealize Automation certificates without completing this procedure, the vRealize Orchestrator Control Center may be inaccessible, and errors may appear in the vco-server and vco-configurator log files.

Problems with updating certificates can also occur if vRealize Orchestrator is configured to authenticate against a different tenant and group than vRealize Automation. See https://kb.vmware.com/kb/2147612.

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.
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.x environment, you must update the URL of the infrastructure endpoint that points to the target embedded vRealize Orchestrator server.

Prerequisites

- Successfully migrate to vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://*vra-va-hostname.domain.name*/vcac.

     For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://*vra-va-lb-hostname.domain.name*/vcac.
  b. Log in as a IaaS administrator user.

Procedure

1. Select **Infrastructure > Endpoints > Endpoints**.
2. On the Endpoints page, select the vRealize Orchestrator endpoint, and click **Edit**.
3. In the Address text box, edit the vRealize Orchestrator endpoint URL.
   - If you migrated to a minimal environment, replace the vRealize Orchestrator endpoint URL with `https://vra-va-hostname.domain.name:443/vco`.
   - If you migrated to a high-availability environment, replace the vRealize Orchestrator endpoint URL with `https://vra-va-lb-hostname.domain.name:443/vco`.
4. Click **OK**.
5. Manually run a data collection on the vRealize Orchestrator endpoint.
   a. On the Endpoints page, select the vRealize Orchestrator endpoint.
   b. Select**Actions > Data Collection**.

   Verify that the data collection is successful.

Reconfigure the Azure Endpoint in the Target vRealize Automation Environment

After migration, you must reconfigure your Microsoft Azure endpoint.

Perform this procedure for each Azure endpoint.

Prerequisites

- Successfully migrate to the latest version of vRealize Automation 7.4.
- Log in to the target vRealize Automation console.
  a. Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://*vra-va-hostname.domain.name*/vcac.

     For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://*vra-va-lb-hostname.domain.name*/vcac.
  b. Log in as a IaaS administrator user.

Procedure

1. Select **Administration > vRO Configuration > Endpoints**.
2. Select an Azure endpoint.
3. Click **Edit**.
4. Click **Details**.
5. In the **Client secret** text box, enter the original client secret.
6. Click **Finish**.
7. Repeat for each Azure endpoint.

Migrate vRealize Automation 6.2.x Automation Application Services to 7.4

You can use the VMware vRealize Application Services Migration Tool to migrate your existing application services blueprints and deployment profiles from VMware vRealize Application Services 6.2.x to vRealize Automation 7.4.

Prerequisites

Successful migration to the latest version of vRealize Automation.

Procedure

- To download the VMware vRealize Application Services Migration Tool, complete these steps.
  a. Click Download VMware vRealize Automation.
  b. Select **Drivers & Tools > VMware vRealize Application Services Migration Tool**.

Delete Original Target vRealize Automation IaaS Microsoft SQL Database

You can delete the original IaaS database after migration is complete.

Prerequisites

Successful migration to the latest version of vRealize Automation.

Your migrated environment does not use the original vRealize Automation IaaS Microsoft SQL database that you created when you installed the target vRealize Automation environment. You can safely delete this original IaaS database from the Microsoft SQL Server after you complete migration.

Update Data Center Location Menu Contents After Migration

After migration, you must add any missing custom data center locations to the **Location** drop-down menu.

After migration to the latest version of vRealize Automation, the data center locations in the **Location** drop-down menu on the Compute Resources page revert to the default list. Although custom data center locations are missing, all compute resource configurations migrate successfully and the `Vrm.DataCenter.Location` property is not affected. You can still add custom data center locations to the **Location** menu.

Prerequisites

Migrate to the latest version of vRealize Automation.

Procedure

- Add missing data center locations to the **Location** drop-down menu. See *Scenario: Add Datacenter Locations for Cross Region Deployments* in *Configuring vRealize Automation*.

Upgrading Software Agents to TLS 1.2

After you migrate to vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4, you must perform several tasks to upgrade the Software Agents from your source environment to Transport Layer Security (TLS) 1.2

Beginning with vRealize Automation 7.4, TLS 1.2 is the only supported TLS protocol for data communication between vRealize Automation and your browser. After migration, you must upgrade existing virtual machine templates from your vRealize Automation 7.1 or 7.3 source environment as well as any existing virtual machines.

Update Source Environment Virtual Machine Templates

You must update existing vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 templates after you complete migration to 7.4 so that the Software Agents use the TLS 1.2 protocol.

Guest agent and agent bootstrap code must be updated in the source environment templates. If you are using a linked clone option, you might need to remap the templates with the newly created virtual machines and their snapshots.

To upgrade your templates, you complete these tasks.

1 Log in to vSphere.

2 Convert each template from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to a virtual machine and power on the machine.

3 Import the appropriate software installer and run the software installer on each virtual machine.

4 Convert each virtual machine back to a template.

Use this procedure to locate the software installers for Linux or Windows.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.

Procedure

1 Start a browser and open the vRealize Automation 7.4 appliance splash page using the fully qualified domain name of the virtual appliance: https://*vra-va-hostname.domain.name*.

2 Click **Guest and software agents page**.

3 Follow the instructions for the Linux or Windows software installers.

What to do next

Identify Virtual Machines that Need Software Agent Upgrade.

Identify Virtual Machines that Need Software Agent Upgrade

You can use the Health Service in the vRealize Automation Console to identify virtual machines that need software agent update to TLS 1.2.

Sometimes the patch applied to your vRealize Automation source environment does not upgrade all of the virtual machines. You can use the Health Service to identify the virtual machines that still need a software agent update to TLS 1.2. All software agents in the target environment need to be updated for post-provisioning procedures.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- You have successfully migrated vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You are logged in to vRealize Automation 7.4 on the primary virtual appliance.

Procedure

1 Click **Administration > Health**.

2 Click **New Configuration**.

3 On the Configuration Details page, provide the requested information.

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 6-1. 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 6-2. vRealize Automation System Tenant

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

Table 6-3. vRealize Automation Disk Space Monitoring

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

Table 6-4. 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 any outdated Software Agents on vSphere to TLS 1.2 after migration using vRealize Automation Appliance Management.

This procedure updates the outdated Software Agents on the virtual machines from your source environment to TLS 1.2 and is required for migration to vRealize Automation 7.4.

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- You have used Health Service to identify virtual appliances with outdated Software Agents.

Procedure

1 On your primary vRealize Automation appliance, log in to vRealize Automation Appliance Management as **root** using the password you entered when you deployed the vRealize Automation appliance.

For a high-availability environment, open Appliance Management on the master appliance.

2 Click **vRA Settings > SW Agents**.

3 Click **Toggle TLS 1.0, 1.1**.

TLS v1.0, v1.1 Status is ENABLED.

4 For Tenant credentials, enter the requested information for the source vRealize Automation appliance.

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 Azure

You can upgrade outdated Software Agents on Amazon Web Service (AWS) or Azure manually.

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

Prerequisites

- Apply Software Agent Patch if you migrated from vRealize Automation 7.1, or 7.3 to 7.4.
- Successful migration from vRealize Automation 7.1, 7.2, 7.3 or 7.3.1 to 7.4.
- A software tunnel is present and the tunnel virtual machine IP address is known.

Procedure

1 Create a node file for each node that you need to upgrade.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py –a <
$DestinationVRAServer> –t <$Tenant> –tu <$TenantUser> –S <$SourceVRAServer>
```

2 Create a plan file to upgrade the Software Agent on a Linux or a Windows virtual machine.

- Modify the migrate params file under /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} to contain the value of the private IP address corresponding to the AWS or Azure endpoint.

```
"key": "ipAddress",

        "value": {

            "type": "string",

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

        }
```

- Use this command for updating a Linux machine.

```
/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.

Validate the Target vRealize Automation 7.4 Environment

You can verify that all data is migrated successfully to the target vRealize Automation environment.

Prerequisites

- Migrate to the latest version of vRealize Automation.
- Log in to the target vRealize Automation console.
  a Open the vRealize Automation console using the fully qualified domain name of the target virtual appliance: https://*vra-va-hostname.domain.name*/vcac.

    For a high-availability environment, open the console using the fully qualified domain name of the target virtual appliance load balancer: https://*vra-va-lb-hostname.domain.name*/vcac.

  b Log in with the tenant administrator user name and password.

Procedure

1. Select **Infrastructure > Managed Machines** and verify that all the managed virtual machines are present.
2. Click **Compute Resources**, select each endpoint, and click **Data Collection**, **Request now**, and **Refresh** to verify that the endpoints are working.
3. Click **Design**, and on the **Blueprints** page, verify the elements of each blueprint.
4. Click **XaaS** and verify the contents of **Custom Resources**, **Resource Mappings**, **XaaS Blueprints**, and **Resource Actions**.
5. Select **Administration > Catalog Management** and verify the contents of **Services**, **Catalog Items**, **Actions**, and **Entitlements**.
6. Select **Items > Deployments** and verify the details for the provisioned virtual machines.
7. On the Deployments page, select a provisioned, powered off, virtual machine and select **Actions > Power On**, click **Submit**, and click **OK**. Verify that the virtual machine powers on correctly.
8. Click **Catalog** and request a new catalog item.
9. On the **General** tab, enter the request information.
10. Click the Machine icon, accept all the default settings, click **Submit**, and click **OK**.
11. Verify that the request finishes successfully.

Troubleshooting Migration

7

Migration troubleshooting topics provide solutions to problems you might experience when you migrate vRealize Automation.

This chapter includes the following topics:

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 7-1. Source vRealize Automation Appliance

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

Table 7-2. 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 7-3. 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.

Note Server Logs

- Tail the updateSoftwareAgents.log file on the server to observe the process: /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log.
- Tail the catlaina.out file on target appliance to see which software agents are succeeding: /var/log/vcac/catalina.out.

  Look for s string such as "ping" reported back for 7.4.0-SNAPSHOT.

You can find additional information at these locations.

- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan
- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log
- /var/cache/vcac/agentupdate/sqa/UUID/UUID.log (per OS)

Before you start a major batch upgrade, you should always perform a test virtual appliance software agent upgrade. For an overview of the process:

- Observe the first request made to the target virtual appliance to identify the agent versions.
- Observe the request made to the source virtual appliance for upgrade.
- Observe the agents reporting their new 7.4 version in the target virtual appliance.
- Between these events, observe the updateSoftwareAgents.log file at /storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log

Note Client Logs

Linux agent logs are in appdirector agent logs folder: /opt/vmware-appdirector/agent/logs/*.log

You might see log errors like these, which are temporary because the EBS queues go out and in during the upgrade process.

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

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

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

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

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

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

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

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