Upgrading from vRealize Automation 7.1 or Later 7.x to 7.5

25 January 2019
vRealize Automation 7.5

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

Contents

Updated Information

The following table lists the changes to *Upgrading from vRealize Automation 7.1 and later* for this product release.

This table provides the update history of *Upgrading from vRealize Automation 7.1 and later*.

Revision	Description
25 JAN 2019	Minor updates.
13 NOV 2018	Updates to the Migrating vRealize Orchestrator After Upgrading vRealize Automation section. Included external links from vRealize Orchestrator to vRealize Automation documentation.
04 OCT 2018	Minor updates.
20 SEP 2018	Initial document release.

Upgrading from vRealize Automation 7.1.x

1

You can upgrade vRealize Automation 7.1.x to this vRealize Automation release. You use upgrade procedures specific to this version to upgrade your environment.

An in-place upgrade is a three-stage process. You upgrade the components in your current environment in this order.

1 vRealize Automation appliance

2 IaaS web server

3 Migrate vRealize Orchestrator

You must upgrade all product components to the same version.

Beginning with vRealize Automation 7.2, JFrog Artifactory Pro is no longer bundled with the vRealize Automation appliance. If you upgrade from an earlier version of vRealize Automation, the upgrade process removes JFrog Artifactory Pro. For more information, see Knowledge Base 2147237.

This chapter includes the following topics:

- Prerequisites for Upgrading vRealize Automation

- Checklist for Upgrading vRealize Automation

- vRealize Automation Environment User Interfaces

Prerequisites for Upgrading vRealize Automation

Before you run start the vRealize Automation upgrade process, review these prerequisites.

System Configuration Requirements

Verify that the following prerequisites are finished before you begin an upgrade.

- Verify that all appliances and servers that are part of your deployment meet the system requirements for the latest version. See the vRealize Automation support matrix link at vRealize Automation product documentation.

- Consult the *VMware Product Interoperability Matrix* on the VMware website for information about compatibility with other VMware products. See the vRealize Automation interoperability matrices link at vRealize Automation product documentation.

- Verify that the vRealize Automation you are upgrading from is in stable working condition. Correct any problems before upgrading.

- Verify that you have changed the load balancer timeout settings from default to at least 10 minutes.

Hardware Configuration Requirements

Verify that the hardware in your environment is adequate for vRealize Automation the release that you are upgrading to.

See *vRealize Automation Hardware Specifications and Capacity Maximums* in Reference Architecture in the vRealize Automation documentation.

Verify that the following prerequisites are finished before you begin an upgrade.

- You must have at least 18 GB RAM, 4 CPUs, Disk1=50 GB, Disk3=25 GB, and Disk4=50 GB before you run the upgrade.

  If the virtual machine is on vCloud Networking and Security, you might need to allocate more RAM space.

  Although general support for vCloud Networking and Security has ended, the VCNS custom properties continue to be valid for NSX purposes. See the Knowledge Base article 2144733.

- These nodes must have at least 5 GB of free disk space:

  - Primary IaaS Website

  - Microsoft SQL database

  - Model Manager

- The primary IaaS Website node where the Model Manager data is installed must have JAVA SE Runtime Environment 8, 64 bits, update 181 or later installed. After you install Java, you must set the JAVA_HOME environment variable to the new version.

- To download and run the upgrade, you must have the following resources:

  - At least 15 GB on the root partition

  - 5 GB on the `/storage/db` partition for the master vRealize Automation appliance

  - 15 GB on the root partition for each replica virtual appliance

- Check the `/storage/log` subfolder and remove any older archived ZIP files to clean up space.

General Prerequisites

Verify that the following prerequisites are finished before you begin an upgrade.

- You have access to all databases and all load balancers impacted by or participating in the vRealize Automation upgrade.

- You make the system unavailable to users while you perform the upgrade.

- You disable any applications that query vRealize Automation.

- Verify that Microsoft Distributed Transaction Coordinator (MSDTC) is enabled on all vRealize Automation and associated SQL servers. For instructions, see Knowledge Base article 2089503.

- Complete these steps if you are upgrading a distributed environment configured with an embedded PostgreSQL database.

  a   Examine the files in the `pgdata` directory on the master host before you upgrade the replica hosts.

  b   Navigate to the PostgreSQL data folder on the master host at `/var/vmware/vpostgres/current/pgdata/`.

  c   Close any opened files in the `pgdata` directory and remove any files with a .swp suffix.

  d   Verify that all files in this directory have correct ownership: postgres:users.

- If you use the DynamicTypes plugin, export the vRealize Orchestrator DynamicTypes plug-in configuration as a package.

  a   Log in to the Java Client as an administrator user.

  b   Select the **Workflows** tab.

  c   Select **Library** > **Dynamic Types** > **Configuration**.

  d   Select the **Export Configuration as Package** workflow and run it.

  e   Click **Not Set** > **Insert value**.

  f   Select the namespaces you want to export and click **Add** to add them to the package.

  g   Click **Submit** to export the package.

In addition, verify that custom properties do not have spaces in their names. Before upgrading to this release of vRealize Automation, remove any space characters from your custom property names, for example replace the space with an underscore character, to allow the custom property to be recognized in the upgraded vRealize Automation installation. vRealize Automation custom property names cannot contain spaces. This issue can impact use of an upgraded vRealize Orchestrator installation that uses custom properties that contained spaces in earlier releases of either vRealize Automation or vRealize Orchestrator or both.

Checklist for Upgrading vRealize Automation

When you upgrade from vRealize Automation 7.x or later, you update all vRealize Automation components in a specific order.

The order of upgrade varies depending on whether you are upgrading a minimal environment or a distributed environment with multiple vRealize Automation appliances.

Use the checklists to track your work as you complete the upgrade. Finish the tasks in the order they are given.

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

Task	Instructions
☐ Run NSX network and security inventory data collection before you upgrade. This is only required when vRealize Automation is integrated with NSX.	See Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.
☐ Backup your current installation. This is a critical step.	For more information on how to back up and restore your system, see Back Up Your Existing vRealize Automation Environment. For general information, see *Configuring Backup and Restore by Using Symantec Netbackup* at http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf.
☐ Download update to the vRealize Automation appliance.	See Downloading vRealize Automation Appliance Updates.
☐ Install the update on the vRealize Automation appliance and IaaS components.	See Install the Update on the vRealize Automation Appliance and IaaS Components

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

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

vRealize Automation Environment User Interfaces

You use and manage your vRealize Automation environment with several interfaces.

User Interfaces

These tables describe the interfaces that you use to manage your vRealize Automation environment.

Table 1-3. vRealize Automation Administration Console

Purpose	Access	Required Credentials
You use the vRealize Automation console for these system administrator tasks. ■ Add tenants. ■ Customize the vRealize Automation user interface. ■ Configure email servers. ■ View event logs. ■ Configure vRealize Orchestrator.	1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://*vrealize-automation-appliance-FQDN*. 2 Click **vRealize Automation console**. You can also use this URL to open the vRealize Automation console: https://*vrealize-automation-appliance-FQDN*/vcac 3 Log in.	You must be a user with the system administrator role.

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

Purpose	Access	Required Credentials
You use vRealize Automation for these tasks. ■ Request new IT service blueprints. ■ Create and manage cloud and IT resources. ■ Create and manage custom groups. ■ Create and manage business groups. ■ Assign roles to users.	1 Start a browser and enter the URL of your tenancy using the fully qualified domain name of the virtual appliance and the tenant URL name: https://*vrealize-automation-appliance-FQDN*/vcac/org/*tenant_URL_name* . 2 Log in.	You must be a user with one or more of these roles: ■ Application Architect ■ Approval Administrator ■ Catalog Administrator ■ Container Administrator ■ Container Architect ■ Health Consumer ■ Infrastructure Architect ■ Secure Export Consumer ■ Software Architect ■ Tenant Administrator ■ XaaS Architect

Table 1-5. vRealize Automation Appliance Management Interface.

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://*vrealize-automation-appliance-FQDN* 2 Click **vRealize Automation Appliance Management**. You can also use this URL to open the vRealize Automation appliance management interface: https://*vrealize-automation-appliance-FQDN*:5480 3 Log in.	▪ User name: root ▪ Password: Password you entered when you deployed the vRealize Automation appliance.

Table 1-6. vRealize Orchestrator Client

Purpose	Access	Required Credentials
You use the vRealize Orchestrator Client for these tasks. ▪ Develop actions. ▪ Develop workflows. ▪ Manage policies. ▪ Install packages. ▪ Manage user and user group permissions. ▪ Attach tags to URI objects. ▪ View inventory.	1 Start a browser and open the vRealize Automation splash page using the fully qualified domain name of the virtual appliance: https://*vrealize-automation-appliance-FQDN* 2 To download the client.jnlp file to your local computer, click **vRealize Orchestrator Client**. 3 Right-click the `client.jnlp` file and select **Launch**. 4 On the Do you want to Continue? dialog box, click **Continue**. 5 Log in.	You must be a user with the system administrator role or part of the vcoadmins group configured in the vRealize Orchestrator Control Center Authentication Provider settings.

Table 1-7. vRealize Orchestrator Control Center

Purpose	Access	Required Credentials
You use the vRealize Orchestrator Control Center to edit the configuration of the default vRealize Orchestrator instance that is embedded in vRealize Automation.	1 Start a browser and open the vRealize Automation appliance splash page using the fully qualified domain name of the virtual appliance: https://*vrealize-automation-appliance-FQDN* 2 Click **vRealize Automation Appliance Management**. You can also use this URL to open the vRealize Automation appliance management interface: https://*vrealize-automation-appliance-FQDN*:5480 3 Log in. 4 Click **vRA > Orchestrator**. 5 Select **Orchestrator user interface**. 6 Click **Start**. 7 Click the Orchestrator user interface URL. 8 Log in.	User Name ■ Enter **root** if role-based authentication is not configured. ■ Enter your vRealize Automation user name if it is configured for role-based authentication. Password ■ Enter the password you entered when you deployed the vRealize Automation appliance if role-based authentication is not configured. ■ Enter the password for your user name if your user name is configured for role-based authentication.

Table 1-8. Linux Command Prompt

Purpose	Access	Required Credentials
You use the Linux command prompt on a host, such as the vRealize Automation appliance host, for these tasks. ■ Stop or start services ■ Edit configuration files ■ Run commands ■ Retrieve data	1 On the vRealize Automation appliance host, open a command prompt. One way to open the command prompt on your local computer is to start a session on the host using an application such as PuTTY. 2 Log in.	■ User name: root ■ Password: Password you created when you deployed the vRealize Automation appliance.

Table 1-9. Windows Command Prompt

Purpose	Access	Required Credentials
You can use a Windows command prompt on a host, such as the IaaS host, to run scripts.	1 On the IaaS host, log in to Windows. One way to log in from your local computer is to start a remote desktop session. 2 Open the Windows command prompt. One way to open the command prompt is to right-click the Start icon on the host and select **Command Prompt** or **Command Prompt (Admin)**.	■ User name: User with administrative privileges. ■ Password: User's password.

Upgrading VMware Products Integrated with vRealize Automation

2

You must manage any VMware products integrated with your vRealize Automation environment when you upgrade vRealize Automation.

If your vRealize Automation environment is integrated with one or more additional products, you should upgrade vRealize Automation before you update the additional products. If vRealize Business for Cloud is integrated with vRealize Automation, you must unregister vRealize Business for Cloud before you upgrade vRealize Automation.

Follow the suggested workflow for managing integrated products when you upgrade vRealize Automation.

1   Upgrade vRealize Automation.

2   Upgrade VMware vRealize Operations Manager.

3   Upgrade VMware vRealize Log Insight.

4   Upgrade VMware vRealize Business for Cloud.

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

This chapter includes the following topics:

- Upgrading vRealize Operations Manager Integrated with vRealize Automation

- Upgrading vRealize Log Insight Integrated with vRealize Automation

- Upgrading vRealize Business for Cloud Integrated with vRealize Automation

Upgrading vRealize Operations Manager Integrated with vRealize Automation

Upgrade vRealize Operations Manager after you upgrade vRealize Automation.

Procedure

1   Upgrade vRealize Automation.

2   Upgrade vRealize Operations Manager. For information, see *Updating Your Software* in the VMware vRealize Operations Manager Documentation.

Upgrading vRealize Log Insight Integrated with vRealize Automation

Upgrade vRealize Log Insight after you upgrade vRealize Automation.

Procedure

1   Upgrade vRealize Automation.

2   Upgrade vRealize Log Insight. For information, see *Upgrading vRealize Log Insight* in the VMware vRealize Log Insight Documentation.

Upgrading vRealize Business for Cloud Integrated with vRealize Automation

When you upgrade your vRealize Automation environment, you must unregister and register your connection to vRealize Business for Cloud.

Perform this procedure to ensure continuity of service with vRealize Business for Cloud when you upgrade your vRealize Automation environment.

Procedure

1   Unregister vRealize Business for Cloud from vRealize Automation. See *Unregister vRealize Business for Cloud from vRealize Automation* in the vRealize Business for Cloud Documentation.

2   Upgrade vRealize Automation.

3   If necessary, upgrade vRealize Business for Cloud for Cloud. See *Upgrading vRealize Business for Cloud* in the vRealize Business for Cloud Documentation.

4   Register vRealize Business for Cloud with vRealize Automation. See *Register vRealize Business for Cloud with vRealize Automation* in the vRealize Business for Cloud Documentation.

Preparing to Upgrade vRealize Automation

3

Complete these tasks before you upgrade from vRealize Automation 7.x.

Complete these tasks in the order they appear in the checklist. See Checklist for Upgrading vRealize Automation.

This chapter includes the following topics:

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

Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation

Before you upgrade vRealize Automation 7.1 or later, you must run NSX Network and Security Inventory data collection in your the source vRealize Automation 7.1 or later environment that you are upgrading from.

This data collection is required for the load balancer reconfigure action to work in vRealize Automation your deployments.

Procedure

- ◆ Run NSX Network and Security Inventory data collection in the source vRealize Automation 7.1 or later environment that you are upgrading from before you start the upgrade. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation*.

What to do next

Backup Prerequisites for Upgrading vRealize Automation.

Backup Prerequisites for Upgrading vRealize Automation

Complete the backup prerequisites before you begin your upgrade.

Prerequisites

- Verify that your source environment is fully installed and configured.

- Log in to your vSphere client and for each appliance in your source environment, back up all the vRealize Automation appliance configuration files in the following directories:

    - `/etc/vcac/`

    - `/etc/vco/`

    - `/etc/apache2/`

    - `/etc/rabbitmq/`

- Back up the IaaS Microsoft SQL Server database. For information, find articles on the Microsoft Developer Network about creating a full SQL Server database backup.

- Back up any files you have customized, such as `DataCenterLocations.xml`.

- Create a snapshot of each virtual appliance and IaaS server. Adhere to regular guidelines for backing up the entire system in case vRealize Automation upgrade is unsuccessful. See *Backup and Recovery for vRealize Automation Installations* in *Managing vRealize Automation*.

Back Up Your Existing vRealize Automation Environment

If an update is unsuccessful, use the snapshot to return to the last known good configuration and attempt another upgrade.

Prerequisites

Before you upgrade from vRealize Automation 7.1 or later, shut down and take a snapshot of each vRealize Automation IaaS server on each Windows node and each vRealize Automation appliance on each Linux node.

- Backup Prerequisites for Upgrading vRealize Automation.

- The PostgreSQL database is configured in high-availability mode. Log in to the vRealize Automation appliance management interface and select **Cluster** to locate the current Master node. If the database configuration is listed as an external database, create a manual backup of this external database.

- If the vRealize Automation Microsoft SQL database is not hosted on the IaaS server, create a database backup file.

- Verify that you have completed the backup prerequisites for upgrading.

- Verify that you have taken a snapshot of your system while it is shut down. This is the preferred method of taking a snapshot. For information about creating and managing snapshots, see vSphere product documentation.

    Note   When you back up the vRealize Automation appliance and the IaaS components, disable in-memory snapshots and quiesced snapshots.

- If you modified any of the *.exe.config (e.g. managerservice.exe.config) files on your IaaS servers, make a backup of that file. See Restore Changes to Logging in the app.config File.

- Make a backup of the external workflow configuration (xmldb) files. See Restore External Workflow Timeout Files.

- Verify that you have a location outside your current folder where you can store your backup file. See Backup Copies of .xml Files Cause the System to Time Out.

Procedure

1   Log in to your vSphere client.

2   Locate each vRealize Automation IaaS Windows machine, and each vRealize Automation appliance node.

3   To preserve data integrity you must shut down in a specific order. If you are using vCenter Server to manage your virtual machines, use the guest `shutdown` command to shut down vRealize Automation. See *Shut Down vRealize Automation* in the *Managing vRealize Automation* PDF in vRealize Automation product documentation.

4   Take a snapshot of each vRealize Automation machine.

5   Use your preferred backup method to create a full backup of each appliance node.

6   When you start vRealize Automation from the beginning, such as after a power outage, a controlled shutdown or after recovery, you must start the components in a specified order. For information, see *Start Up vRealize Automation* in the *Managing vRealize Automation* PDF in vRealize Automation product documentation.

7   Log in to each vRealize Automation appliance management console and verify that the system is fully functional.

   a   Click **Services**.

   b   Verify that each service is REGISTERED.

What to do next

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous

If you upgrade from a distributed vRealize Automation environment that operates in PostgreSQL synchronous replication mode, you must change it to asynchronous before you upgrade.

Prerequisites

You have a distributed vRealize Automation environment that you want to upgrade.

Procedure

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

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

2   Click **Cluster**.

3   Click **Async Mode** and wait until the action completes.

4   Verify that all nodes in the Sync State column display `Async` status.

What to do next

Downloading vRealize Automation Appliance Updates

Downloading vRealize Automation Appliance Updates

You can check for updates on your vRealize Automation appliance management interface, and download the updates using one of the following methods.

For best upgrade performance, use the ISO file method.

To avoid potential problems when upgrading your appliance, or if issues arise during appliance upgrade, see VMware Knowledge Base article *vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database (54987)*.

Download Virtual Appliance Updates for Use with a CD-ROM Drive

You can update your virtual appliance from an ISO file that the appliance reads from the virtual CD-ROM drive. This is the preferred method.

You download the ISO file and set up the primary appliance to use this file to upgrade your appliance.

Prerequisites

■   Back up your existing vRealize Automation envrionment.

■   Verify that all CD-ROM drives you use in your upgrade are enabled before you update a vRealize Automation appliance. See the vSphere documentation for information about adding a CD-ROM drive to a virtual machine in the vSphere client.

Procedure

1   Download the update repository ISO file.

    a   Start a browser and go to the vRealize Automation product page at www.vmware.com.

    b   Click **vRealize Automation Download Resources** to go to the VMware download page.

    c   Download the appropriate file.

2   Locate the downloaded file on your system to verify that the file size is the same as the file on the VMware download page. Use the checksums provided on the download page to validate the integrity of your downloaded file. For information, see the links at the bottom of the VMware download page.

3   Verify that your primary virtual appliance is powered on.

4   Connect the CD-ROM drive for the primary virtual appliance to the ISO file you downloaded.

> **Note**   Log in to the appliance and mount the CD-ROM within Linux using this file path
> `mount /dev/sr0 /media/cdrom` if you are unable to see the update after the ISO file attaches to
> the virtual machine.

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

6   Click the **Update** tab.

7   Click **Settings**.

8   Under Update Repository, select **Use CDROM Updates**.

9   Click **Save Settings**.

Download vRealize Automation Appliance Updates from a VMware Repository

You can download the update for your vRealize Automation appliance from a public repository on the
vmware.com website.

Prerequisites

- Back up your existing vRealize Automation environment.

- Verify that your vRealize Automation appliance is powered on.

Procedure

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

2   Click the **Update** tab.

3   Click **Settings**.

4   (Optional) Set how often to check for updates in the Automatic Updates panel.

5   Select **Use Default Repository** in the Update Repository panel.

    The default repository is set to the correct VMware.com URL.

6   Click **Save Settings**.

Updating the vRealize Automation Appliance and IaaS Components

4

After you finish the upgrade prerequisites and download the virtual appliance update, you install the update.

For a minimal environment, you install the update on the vRealize Automation appliance. For a distributed environment, you install the update on the master appliance node. The time required for the update to finish varies according to your environment and network. When the update finishes, the system displays the changes made on the Update Status page of vRealize Automation Appliance Management. When the appliance update finishes, you must reboot the appliance. When you reboot the master appliance in a distributed environment, the system reboots each replica node.

After you reboot, `Waiting for VA services to start` appears on the Update Status page. The IaaS update starts when the system is fully initialized and all services are running. You can observe the IaaS upgrade progress on the Update Status page. The first IaaS server component can take about 30 minutes to finish. During the upgrade, you see a message similar to `Upgrading server components for node web1-vra.mycompany.com`.

At the end of the upgrade process for each Manager Service node, you see a message similar to `Enabling ManagerService automatic failover mode for node mgr-vra.mycompany.com`. Beginning with vRealize Automation 7.3, the active Manager Service node changes from a manual election to a system decision about which node becomes the failover server. The system enables this feature during upgrade. If you have problems with this feature, see Update Fails to Upgrade the Management Agent.

Install the Update on the vRealize Automation Appliance and IaaS Components

You install the update on the source vRealize Automation virtual appliance to upgrade vRealize Automation and the IaaS components to the target vRealize Automation release.

Do not close the vRealize Automation appliance management interface while you install the update.

If you encounter any problems during the upgrade process, see Chapter 9 Troubleshooting the vRealize Automation Upgrade.

Note   While upgrading the Management Agent on the IaaS virtual machines, a VMware public certificate is temporarily installed in your Trusted Publishers certificate store. The Management Agent upgrade process uses a PowerShell script that is signed with this certificate. When the upgrade is finished, this certificate is removed from your certificate store.

Prerequisites

- Verify that you selected a download method and have finished the procedure for the method. See Downloading vRealize Automation Appliance Updates.

- For all high-availability environments, see Back Up Your Existing vRealize Automation Environment.

- For environments with load balancers, verify that you disabled all the redundant nodes and removed the health monitors. For information, see your load balancer documentation.

  - vRealize Automation appliance

  - IaaS Website

  - IaaS Manager Service

  Note   When performing an automatic upgrade from vRealize Automation 7.4 or later, you do not need to disable secondary IaaS web load balancer monitors. Do not disable IaaS Manager Server load balancer monitors before upgrade. If you are upgrading IaaS nodes manually by using the legacy IaaS installer, you must disable traffic for the secondary web nodes before the upgrade.

- For environments with load balancers, verify that the traffic is directed only to the primary node.

- Verify that the IaaS service hosted in Microsoft Internet Information Services (IIS) is running by performing the following steps:

  a   Start a browser and enter the URL **https://*webhostname*/Repository/Data/MetaModel.svc** to verify that the Web Repository is running. If successful, no errors are returned and you see a list of models in XML format.

  b   Log in to the IaaS Website and check that the status recorded in the `Repository.log` file reports OK. The file is located in the VCAC home folder at `/Server/Model Manager Web/Logs/Repository.log`.

  Note   For a distributed IaaS Website, log in to the secondary website, without MMD, and stop Microsoft IIS temporarily. To ensure that the load balancer traffic is only going through the primary Web node, select the MetaModel.svc connectivity, and restart the Microsoft IIS.

- Verify that all IaaS nodes are in a healthy state by performing the following steps:

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

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

    b   Select **Cluster**.

    c   Under **Last Connected**, verify the following.

- The IaaS nodes in the table have a last connected time of less than 30 seconds.

- The virtual appliance nodes have a last connected time of less than 10 minutes.

       If the IaaS nodes are not in communication with the vRealize Automation appliance, the upgrade fails.

       To diagnose connectivity problems between the Management Agent and virtual appliance, perform these steps.

       1   Log in to each IaaS node that is not listed or has a **Last Connected** time greater than 30 seconds.

       2   Check the Management Agent logs to see if any errors are recorded.

       3   If the Management Agent is not running, restart the agent in the Services console.

    d   Note any orphaned nodes listed in the table. An orphaned node is a duplicate node that is reported on the host but does not exist on the host. You must delete all orphaned nodes. For more information, see Delete Orphaned Nodes on vRealize Automation.

- If you have a replica virtual appliance that is no longer part of the cluster, you must delete it from the cluster table. If you do not delete this appliance, the upgrade process displays a warning message that the replica update is unsuccessful.

- Verify that all saved and in-progress requests have finished successfully before you upgrade.

- If you upgrade the IaaS components manually after you update the vRealize Automation source appliance, see Exclude IaaS Upgrade. If you plan to upgrade IaaS manually, you must also stop all IaaS services, except Management Agent, on each IaaS node.

Procedure

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

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

2   Click **Services** and verify that all services are registered.

3   Select **Cluster** and verify that this appliance is the master vRealize Automation appliance.

    You install the update only on the master vRealize Automation appliance. Each replica vRealize Automation appliance is updated with the master appliance.

4   Select **Update > Status**.

5   Click **Check Updates** to verify that an update is accessible.

6   (Optional) For instances of vRealize Automation appliance, click **Details** in the Appliance Version area to see information about the location of release notes.

7   Click **Install Updates**.

8   Click **OK**.

A message stating that the update is in progress appears. The system shows changes made during an upgrade on the Update Summary page. The time required for the update to finish varies according to your environment and network.

9   (Optional) To monitor the update in greater detail, use a terminal emulator to log in to the primary appliance. View the `updatecli.log` file at `/opt/vmware/var/log/vami/updatecli.log`.

Additional upgrade progress information can also be seen in these files.

- `/opt/vmware/var/log/vami/vami.log`

- `/var/log/vmware/horizon/horizon.log`

- `/var/log/bootstrap/*.log`

If you log out during the upgrade process, you can continue to follow the update progress in the log file. The `updatecli.log` file might display information about the version of vRealize Automation that you are upgrading from. This displayed version changes to the proper version later in the upgrade process.

10   When the vRealize Automation appliance update finishes, click **System > Reboot** in the vRealize Automation appliance management interface.

In a distributed environment, all successfully upgraded replica appliance nodes reboot when you reboot the master appliance.

The IaaS update starts when the system is initialized and all services are up and running. Click **Update > Status** to observe the IaaS upgrade progress.

11   When the IaaS update finishes, click **Cluster** in the vRealize Automation appliance management interface, and verify that the version number is the current version for all IaaS nodes and components.

12   Click **Telemetry** in the vRealize Automation appliance management interface. Read the note about participation in the Customer Experience Improvement Program (CEIP) and select to join or not join the program.

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

For more information about the Customer Experience Improvement Program, see *Join or Leave the Customer Experience Improvement Program for vRealize Automation* in *Managing vRealize Automation*.

What to do next

If your deployment uses a load balancer, perform these steps.

1   Enable the load balancer vRealize Automation health checks.

2   Re-enable the load balancer traffic for all vRealize Automation nodes.

If the IaaS components fail to upgrade, see Chapter 5 Upgrading the IaaS Server Components Separately If the Update Process Fails.

Upgrading the IaaS Server Components Separately If the Update Process Fails

5

If the automatic update process fails, you can upgrade the IaaS components separately.

If the vRealize Automation IaaS Web site and Manager Service successfully upgraded, you can run the IaaS upgrade shell script again without reverting to the snapshots you took before the upgrade. Sometimes a pending reboot event generated while upgrading multiple IaaS components installed on the same virtual machine can fail the upgrade. In this case, try manually rebooting the IaaS node and rerunning the upgrade to fix the problem. If the upgrade fails consistently, contact VMware support or attempt a manual upgrade by following these steps.

1   Revert your vRealize Automation appliance to its pre-update state.

2   Run a command to exclude the IaaS components from the update process. See Exclude IaaS Upgrade.

3   Run the update process on the vRealize Automation appliance.

4   Update the IaaS components separately using the Upgrade Shell Script or the latest release vRealize Automation IaaS installer msi package.

This chapter includes the following topics:

■   Upgrade IaaS Components Using the Upgrade Shell Script After Upgrading the vRealize Automation Appliance

■   Upgrading IaaS Components Using the IaaS Installer Executable File After Upgrading the vRealize Automation Appliance

■   Restore Access to the Built-In vRealize Orchestrator Control Center

Upgrade IaaS Components Using the Upgrade Shell Script After Upgrading the vRealize Automation Appliance

Use the upgrade shell script to upgrade the IaaS components after you update each vRealize Automation 7. 1 or later appliance to the vRealize Automation release that you are upgrading to.

The updated vRealize Automation appliance contains a shell script that you use to upgrade each IaaS node and component.

You can run the upgrade script by using the vSphere console for the virtual machine or by using an SSH console session. If you use the vSphere console, you avoid intermittent network connectivity problems that can break the execution of the script.

If you stop the script while it is upgrading a component, the script stops when it finishes upgrading the component. If other components on the node still must be upgraded, you can run the script again.

When the upgrade finishes, you can review the upgrade result by opening the upgrade log file at `/opt/vmware/var/log/vami/upgrade-iaas.log`.

Prerequisites

- Review Chapter 9 Troubleshooting the vRealize Automation Upgrade.

- Verify the successful update of all vRealize Automation appliances.

- If you reboot an IaaS server after you update all the vRealize Automation appliances but before you upgrade the IaaS components, stop all the IaaS services on Windows, except for the Management Agent service.

- Before you run the upgrade shell script on the master vRealize Automation appliance node, click the **Services** in the vRealize Automation appliance management interface. Verify that each service, except for iaas-service, is REGISTERED.

- To install the IaaS Management Agent manually on each IaaS node, finish these steps.

  a Open a browser to the IaaS Installation page on the appliance.

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

  b Download the Management Agent installer, vCAC-IaaSManagementAgent-Setup.msi.

  c Log in to each vRealize Automation IaaS machine and upgrade the Management Agent with the Management Agent installer. Restart the Windows Management Agent service.

- Verify that your primary IaaS Website and Model Manager node has JAVA SE Runtime Environment 8, 64 bits, update 181 or later installed. After you install Java, you must set the environment variable, JAVA_HOME, to the new version on each server node.

- Log in to each IaaS Website node and verify that the creation date is earlier than the modified date in the `web.config` file. If the creation date for the `web.config` file is the same as or later than the modified date, perform the procedure in Upgrade Fails for IaaS Website Component.

- To verify that each IaaS node has an upgraded IaaS Management Agent, perform these steps on each IaaS node:

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

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

  b Select **Cluster**.

  c Expand the list of all installed components on each IaaS node, and locate the IaaS Management Agent.

  d Verify that the Management Agent version is current.

- Exclude IaaS Upgrade.

- Verify that the IaaS Microsoft SQL Server database backup is accessible in case you must roll back.

■ Verify that snapshots of the IaaS servers in your deployment are available.

If the upgrade is unsuccessful, return to the snapshot and database backup and attempt another upgrade.

Procedure

1 Open a new console session on the vRealize Automation appliance host. Log in with the root account.

2 Change directories to `/usr/lib/vcac/tools/upgrade/`.

It is important that all IaaS Management Agents are upgraded and healthy before running the `./upgrade` shell script. If any IaaS Management Agent has a problem when you run the upgrade shell script, see Update Fails to Upgrade the Management Agent.

3 Run the upgrade script.

a At the command prompt, enter **./upgrade**.

b Press Enter.

For a description of the IaaS upgrade process, see Chapter 4 Updating the vRealize Automation Appliance and IaaS Components.

If the Upgrade Shell Script is unsuccessful, review the `upgrade-iaas.log` file.

You can run the upgrade script again after you fix a problem.

What to do next

1 Restore Access to the Built-In vRealize Orchestrator Control Center.

2 If your deployment uses a load balancer, re-enable the vRealize Automation health monitors and the traffic to all nodes.

For more information, see *vRealize Automation Load Balancing* links in vRealize Automation product documentation.

Upgrading IaaS Components Using the IaaS Installer Executable File After Upgrading the vRealize Automation Appliance

You can use this alternative method to upgrade IaaS components after you upgrade the vRealize Automation 7.1 or later appliance.

Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance

After you upgrade the vRealize Automation appliance to the target release, download the IaaS installer to the machine where the IaaS components to be upgraded are installed.

If you see certificate warnings during this procedure, you can ignore them.

Note   Except for a passive backup instance of the Manager Service, the startup type for all services must be set to Automatic during the upgrade process. If the upgrade process fails set services to Manual.

Prerequisites

- Verify that Microsoft .NET Framework 4.5.2 or later is installed on the IaaS installation machine. You can download the .NET installer from the vRealize Automation installer web page. If you update .NET to 4.5.2 after you shut down the services and the machine restarted as part of the installation, you must manually stop all IaaS services except the Management agent.

- Verify that the .NET 3.5 Framework non-HTTP Activation feature is configured. The vRealize Automation upgrade fails if the .NET 3.5 Framework non-HTTP Activation feature is not set up on all IaaS nodes (web, Manager Service, proxy agent, DEM). The failure occurs if there is no Internet access for the prerequisite checker to download and install the latest .NET version. To add this feature:

  a   Open the **Add Roles and Features Wizard**.

  b   Select **.NET Framework 3.5 Features**.

  c   Select the **non-HTTP activation** check box.

- If you are using Internet Explorer for the download, verify that Enhanced Security Configuration is not enabled. Enter `res://iesetup.dll/SoftAdmin.htm` in the search bar and press Enter.

- Log in as a local administrator to the Windows server. The Windows server is where one or more of the IaaS components you want to upgrade are installed.

Procedure

1   Open a browser to the IaaS Installation page on the primary or master vRealize Automation appliance.

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

2   Click **IaaS installer**.

3   When prompted, save `setup__vrealize-automation-appliance-FQDN@5480.exe` to the desktop.

    Do not change the filename. The name links the installation to the correct vRealize Automation appliance.

What to do next

Upgrade the IaaS Components After Upgrading vRealize Automation to the Target Release.

Upgrade the IaaS Components After Upgrading vRealize Automation to the Target Release

You must upgrade the SQL database and configure all systems that have IaaS components installed. You can use these steps for minimal and distributed installations.

Note The IaaS installer must be on the machine that contains the IaaS components you want to upgrade. You cannot run the installer from an external location, except for the Microsoft SQL database which also can be upgraded remotely from the Web node.

Verify that snapshots of the IaaS servers in your deployment are available. If the upgrade fails, you can return to the snapshot and attempt another upgrade.

Perform the upgrade so that services are upgraded in the following order:

1   IaaS Web sites

    If you are using a load balancer, disable traffic to all non-primary nodes.

    Finish the upgrade on one server before upgrading the next server that is running a Website service. Start with the one that has the Model Manager Data component installed.

    If you are performing a manual external Microsoft SQL database upgrade, you must upgrade the external SQL before you upgrade the Web node. You can upgrade the external SQL remotely from the Web node.

2   Manager Services

    Upgrade the active Manager Service before you upgrade the passive Manager Service.

    If you do not have SSL encryption enabled in your SQL instance, uncheck the SSL encryption checkbox in the Iaas Upgrade configuration dialog box next to the SQL definition.

3   DEM orchestrator and workers

    Upgrade all DEM orchestrators and workers. Finish the upgrade on one server before you upgrade the next server.

4   Agents

    Finish the upgrade on one server before you upgrade the next server that is running an agent.

5   Management Agent

    Is updated automatically as part of the upgrade process.

If you are using different services on one server, the upgrade updates the services in the proper order. For example, if your site has Web site and manager services on the same server, select both for update. The upgrade installer applies the updates in the proper order. You must complete the upgrade on one server before you begin an upgrade on another.

Note If your deployment uses a load balancer, the primary appliance must be connected to the load balancer. All other instances of vRealize Automation appliance appliances must be disabled for load balancer traffic before you apply the upgrade to avoid caching errors.

Prerequisites

- Back up your existing vRealize Automation environment.

- If you reboot an IaaS server after you update all the vRealize Automation appliances but before you upgrade the IaaS components , stop all of the IaaS windows services, except for the Management Agent service, on the server.

- Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance.

- Verify that your primary IaaS Website, Microsoft SQL database, and Model Manager node has JAVA SE Runtime Environment 8, 64bits, update 181 or later installed. After you install Java, you must set the environment variable, JAVA_HOME , to the new version on each server node.

- Verify that the creation date is earlier than the modified date in the `web.config` file. If the creation date for the `web.config` file is the same as or later than the modified date, perform the procedure in Upgrade Fails for IaaS Website Component.

- Complete these steps to reconfigure the Microsoft Distributed Transaction Coordinator (DTC).

  Note Even with Distributed Transaction Coordinator enabled, the distributed transaction might fail if the firewall is turned on.

  a   On the vRealize Automation appliance, select **Start > Administrative Tools > Component Services**.

  b   Expand **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

  c   Choose the appropriate task.

   - For a local standalone DTC, right-click **Local DTC** and select **Properties**.

   - For a clustered DTC expand **Clustered DTCs** and right-click the named clustered DTC and select **Properties**.

  d   Click **Security**.

  e   Select all of the following.

   - **Network DTC Access**

   - **Allow Remote Clients**

- ▪ **Allow Inbound**

- ▪ **Allow Outbound**

- ▪ **Mutual Authentication Required**

  f   Click **OK**.

Procedure

1   If you are using a load balancer, prepare your environment.

   a   Verify the IaaS Website node that contains the Model Manager data is enabled for load balancer traffic.

   You can identify this node by the presence of the `vCAC Folder\Server\ConfigTool` folder.

   b   Disable all other IaaS Websites and non-primary Manager Services for load balancer traffic.

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

3   Click **Next**.

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

5   Type the administrator credentials for your current deployment on the Log In page.

   The user name is `root` and the password is the password that you specified when you deployed the appliance.

6   Select **Accept Certificate**.

7   On the **Installation Type** page, verify that **Upgrade** is selected.

   If **Upgrade** is not selected, the components on this system are already upgraded to this version.

8   Click **Next**.

9   Configure the upgrade settings.

Option	Action
If you are upgrading the Model Manager Data	Select the **Model Manager Data** check box in the vCAC Server section.
	The check box is selected by default. Upgrade the Model Manager data only once. If you are running the setup file on multiple machines to upgrade a distributed installation, the Web servers stop functioning while there is a version mismatch between the Web servers and the Model Manager data. When you have upgraded the Model Manager data and all of the Web servers, all of the Web servers should function.
If you are not upgrading the Model Manager Data	Unselect the **Model Manager Data** check box in the vCAC Server section.

Option	Action
To preserve customized workflows as the latest version in your Model Manager Data	If you are upgrading the Model Manager Data, select the **Preserve my latest workflow versions** check box in the Extensibility Workflows section.
	The check box is selected by default. Customized workflows are always preserved. The checkbox determines version order only. If you used vRealize Automation Designer to customize workflows in the Model Manager, select this option to maintain the most recent version of each customized workflow before upgrade as the most recent version after upgrade.
	If you do not select this option, the version of each workflow provided with vRealize Automation Designer becomes the most recent after upgrade, and the most recent version before upgrade becomes the second most recent.
	For information about vRealize Automation Designer, see *Life Cycle Extensibility*.
If you are upgrading a Distributed Execution Manager or a proxy agent	Enter the credentials for the administrator account in the Service Account section.
	All of the services that you upgrade run under this account.
To specify your Microsoft SQL Server database	If you are upgrading the Model Manager Data, enter the names of the database server and database instance in the **Server** text box in the Microsoft SQL Server Database Installation Information section. Enter a fully qualified domain name (FQDN) for the database server name in the **Database name** text box.
	If the database instance is on a non-default SQL port, include the port number in the server instance specification. The Microsoft SQL default port number is 1433.
	When upgrading the manager nodes, the MSSQL SSL option is selected by default. If your database does not use SSL, uncheck **Use SSL for database connection**.

10 Click **Next**.

11 Confirm that all services to upgrade appear on the Ready to Upgrade page, and click **Upgrade**.

   The Upgrading page and a progress indicator appear. When the upgrade process finishes, the **Next** button is enabled.

12 Click **Next**.

13 Click **Finish**.

14 Verify that all services restarted.

15 Repeat these steps for each IaaS server in your deployment in the recommended order.

16 After all components are upgraded, log in to the vRealize Automation appliance management interface and verify that all services, including IaaS, are now registered.

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

All of the selected components are upgraded to the new release.

What to do next

1   Restore Access to the Built-In vRealize Orchestrator Control Center.

2   If your deployment uses a load balancer, upgrade each load balancer node to use
    vRealize Automation health checks, and re-enable load balancer traffic for any unconnected nodes.

    For more information, see *vRealize Automation Load Balancing*.

Restore Access to the Built-In vRealize Orchestrator Control Center

After you upgrade the IaaS server components, you must restore access to vRealize Orchestrator.

When you upgrade vRealize Automation, you need to perform this procedure to accommodate the recently introduced Role-Based Access Control feature. This procedure is written for a high-availability environment.

Prerequisites

Make a snapshot of your vRealize Automation environment.

Procedure

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

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

2   Select **Cluster**.

3   Identify the master and replica nodes.

4   On each replica node, open an SSH session, log in as administrator, and run this command:

    ```
    service vco-server stop && service vco-configurator stop
    ```

5   On the master node, open an SSH session, log in as administrator, and run this command:

    ```
    rm /etc/vco/app-server/vco-registration-id
    ```

6   On the master node, change directories to `/etc/vco/app-server/`.

7   Open the `sso.properties` file.

8   If the property name `com.vmware.o11n.sso.admin.group.name` contains spaces or any other Bash-related characters that can be accepted as a special character in a Bash command such as an apostrophe (') or a dollar sign ($), complete these steps.

    a   Copy the line with the `com.vmware.o11n.sso.admin.group.name` property and enter `AdminGroup` for the value.

    b   Add # to the beginning of the original line with the `com.vmware.o11n.sso.admin.group.name` property to comment the line.

    c   Save and close the `sso.properties` file.

9   Run this command:

    ```
    vcac-vami vco-service-reconfigure
    ```

10 Open the `sso.properties` file. If the file has changed, complete these steps.

   a   Remove the # from the beginning of the original line with the
        `com.vmware.o11n.sso.admin.group.name` property to uncomment the line.

   b   Remove the copy of the line with the `com.vmware.o11n.sso.admin.group.name` property.

   c   Save and close the `sso.properties` file.

11 Run this command to restart the vco-server service:

   service vco-server restart

12 Run this command to restart the vco-configurator service:

   service vco-configurator restart

13 In the vRealize Automation appliance management interface, click **Services** and wait until all the
   services in the master node are REGISTERED.

14 When all the services are registered, join the vRealize Automation replica nodes to the
   vRealize Automation cluster to synchronize the vRealize Orchestrator configuration.

What to do next

Chapter 6 Migrating an External vRealize Orchestrator After Upgrading vRealize Automation.

Migrating an External vRealize Orchestrator After Upgrading vRealize Automation

<div style="text-align:right">6</div>

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

Note The vRealize Orchestrator instance embedded in vRealize Automation is automatically upgraded with the vRealize Automation upgrade. If you use only an embedded vRealize Orchestrator, then no action is needed.

The vRealize Orchestrator migration transfers an external source vRealize Orchestrator configuration to your newly configured vRealize Orchestrator 7.5 environment, overwriting all existing elements such as workflows, actions, configuration and resource elements, packages, tasks, policies, certificates, plug-ins, and others.

There are two options for migrating an external vRealize Orchestrator when you upgrade to the latest vRealize Automation release.

- Migrate your external vRealize Orchestratorto another external vRealize Orchestrator instance. See Migrating an External to External vRealize Orchestrator 7.5 in the *Migrating vRealize Orchestrator* documentation.

- Migrate your external vRealize Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation. See Migrating an External Orchestrator Server to vRealize Orchestrator 7.5 in the *Migrating vRealize Orchestrator* documentation.

Note The migration of an embedded vRealize Orchestrator instance to an external vRealize Orchestrator environment is not supported.

Enable Your Load Balancers 7

If your deployment uses load balancers, re-enable secondary nodes and health checks and revert the load balancer timeout settings.

The health checks for vRealize Automation vary according to version. For information, see the *vRealize Automation Load Balancing Configuration Guide* in the vRealize Automation Documentation .

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

Post-Upgrade Tasks for Upgrading vRealize Automation

<div style="text-align: right; font-size: 2em;">8</div>

After you upgrade from vRealize Automation 7.1, or later, you must perform required post-upgrade tasks.

This chapter includes the following topics:

- Upgrading Software Agents to TLS 1.2
- Set the vRealize Automation PostgreSQL Replication Mode to Synchronous
- Run Test Connection and Verify Upgraded Endpoints
- Run NSX Network and Security Inventory Data Collection After You Upgrade from vRealize Automation
- Join Replica Appliance to Cluster
- Port Configuration for High-Availability Deployments
- Restore External Workflow Timeout Files
- Restore Changes to Logging in the app.config File
- Reconfigure the Azure Endpoint Post Upgrade
- Enable Automatic Manager Service Failover After Upgrade
- Import DynamicTypes Plug-In

Upgrading Software Agents to TLS 1.2

After you upgrade vRealize Automation, you must perform several tasks to upgrade the Software Agents from your vRealize Automation 7.1 or later environment to TLS 1.2.

Beginning with vRealize Automation 7.4, Transport Layer Security (TLS) 1.2 is the only supported TLS protocol for data communication between vRealize Automation and your browser.

After migration, you must upgrade existing virtual machine templates from your vRealize Automation 7.1 or later environment as well as any existing virtual machines.

Update vRealize Automation Virtual Machine Templates

You must update existing templates after you complete upgrade to the target vRealize Automation release so that the Software Agents use the TLS 1.2 protocol.

Guest agent and agent bootstrap code must be updated in the templates from the source vRealize Automation release. 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 the source vRealize Automation release to a virtual machine and power on the machine.

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

4   Convert each virtual machine back to a template.

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

Prerequisites

Successful upgrade to the target vRealize Automation release.

Procedure

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

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

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

What to do next

Identify Virtual Machines that Need Software Agent Upgrade.

Identify Virtual Machines that Need Software Agent Upgrade

You can use the Health Service in vRealize Automation to identify virtual machines that need a Software Agent update to TLS 1.2.

You can use the Health Service to identify the virtual machines that need a Software Agent update to TLS 1.2. All Software Agents in the vRealize Automation environment need to be updated so that you can perform post-provisioning procedures, which require secure communication between your browser and vRealize Automation.

Prerequisites

- You have successfully upgraded to the vRealize Automation release.

- You are logged in to the target vRealize Automation release on the primary virtual appliance as tenant administrator.

Procedure

1   Click **Administration > Health**.

2   Click **New Configuration**.

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

Option	Comment
Name	Enter `SW Agent verification`.
Description	Add optional description, for example, `Locate software agents for upgrade to TLS 1.2`.
Product	Select the vRealize Automation release that you upgraded or migrated to.
Schedule	Select **None**.

4   Click **Next**.

5   On the Select Test Suites page, select **System Tests for vRealize Automation** and **Tenant Tests for vRealize Automation**.

6   Click **Next**.

7   On the Configure Parameters page, provide the requested information.

Table 8‑1. vRealize Automation Virtual Appliance

Option	Description
Public Web Server Address	- For a minimal deployment, the base URL for the vRealize Automation appliance host. For example, https://*va-host.domain*/. - For a high-availability deployment, the base URL for the vRealize Automation load balancer. For example, https://*load-balancer-host.domain*/.
SSH Console Address	Fully qualified domain name of the vRealize Automation appliance. For example, *va-host.domain*.
SSH Console User	`root`
SSH Console Password	Password for root.
Max Service Response Time (ms)	Accept default: 2000

Table 8‑2. vRealize Automation System Tenant

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

Table 8‑3. vRealize Automation Disk Space Monitoring

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

Table 8-4. vRealize Automation Tenant

Option	Description
Tenant Under Test	Tenant selected for testing.
Fabric Administrator User Name	Fabric administrator user name. For example, admin@va-host.local. **Note** This fabric administrator must also have a tenant administrator and an IaaS administrator role in order for all of the tests to run.
Fabric Administrator Password	Password for fabric administrator.

8   Click **Next**.

9   On the Summary page, review the information and click **Finish**.

    The software agent verification configuration is finished.

10 On the SW Agent verification card, click **Run**.

11 When the test is complete, click the center of the SW Agent verification card.

12 On the SW Agent verification results page, page through the test results and find the Check Software Agent Version test in the Name column. If the test result is Failed, click the **Cause** link in the Cause column to see the virtual machines with an outdated software agent.

What to do next

If you have virtual machines with an outdated software agent, see Upgrade Software Agents on vSphere.

Upgrade Software Agents on vSphere

You can upgrade outdated Software Agents on vSphere to TLS 1.2 after upgrade using vRealize Automation Appliance Management.

This procedure updates the outdated Software Agents to TLS 1.2 on the virtual machines in your upgraded environment. It is required for upgrade to the target vRealize Automation release.

Prerequisites

■   Successful upgrade to the target vRealize Automation release.

■   You have used Health Service to identify virtual appliances with outdated Software Agents.

Procedure

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

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

2   Click **vRA > SW Agents**.

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

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

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

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

5   Click **Test connection**.

If a connection is established, a success message appears.

6   Click **List batches**.

The Batch Choice List table appears.

7   Click **Show**.

A table appears with a list of virtual machines with outdated Software Agents.

8   Upgrade the Software Agent for the virtual machines that are in the UPGRADABLE state.

- To upgrade the Software Agent in an individual virtual machine, click **Show** for a group of virtual machines, identify the virtual machine you want to upgrade and click **Run** to start the upgrade process.

- To upgrade the Software Agent for a batch of virtual machines, identify the group that you want to upgrade and click **Run** to start the upgrade process.

If you have more than 200 virtual machines to upgrade, you can control the batch upgrade process speed by entering values for these parameters.

Option	Description
Batch Size	The number of virtual machines selected for batch upgrade. You can vary this number to adjust the upgrade speed.
Queue Depth	The number of parallel upgrade executions that take place at one time. For example, 20. You can vary this number to adjust the upgrade speed.
Batch Errors	The REST error count causing batch upgrade to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.

Option	Description
Batch Failures	The number of failed Software Agent upgrades causing batch processing to slow down. For example, if you want to stop the current batch upgrade after 5 failures to improve the stability of the upgrade, enter 5 in the text field.
Batch Polling	How often the upgrade process is polled to check the upgrade process. You can vary this number to adjust the upgrade speed.

If the upgrade process is too slow or produces too many unsuccessful upgrades, you can adjust these parameters to improve upgrade performance.

Note Clicking **Refresh** clears the list of batches. It does not affect the upgrade process. It also refreshes information about whether TLS 1.2 is set or not In addition, clicking **Refresh** also performs a health check of vRealize Automation services. If services are not running, the system displays an error message and inactivates all other action buttons.

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

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

Upgrade Software Agents on Amazon Web Service or Azure

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

Prerequisites

- Successful upgrade to your target vRealize Automation release.

- A software tunnel is present and the tunnel virtual machine IP address is known.

Procedure

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

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

Note For an in-place upgrade, the `$DestinationVRAServer` is the same as the `$SourceVRAServer`.

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

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

```
"key": "ipAddress",

        "value": {
```

```
                    "type": "string",

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

              }
```

- Use this command for updating a Linux machine.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestionationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdateversion --
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.WindowsAgentUpdateversion --
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.WindowsAgentUpdateversion --
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.WindowsAgentUpdateversion --
component_linux Software.LinuxAgentUpdate74 --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --
node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action
execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

As you perform this procedure, you can tail logs from the vRealize Automation virtual appliance and host machine to see the Server Agent upgrade process.

After upgrade, the upgrade process imports a software update script for Windows or Linux to the vRealize Automation virtual appliance. You can log into the vRealize Automation virtual appliance host to ensure that the software component is imported successfully. After the component is imported, a software update is sent to the old Event Broker Service (EBS) to relay software update scripts to the identified virtual machines. When the upgrade completes and the new Software Agents become operative, they bind to the new vRealize Automation virtual appliance by sending a ping request.

Note   Useful Log Files

- Catalina output for source vRealize Automation: /var/log/vcac/catalina.out. In this file, you see the upgrade requests being made as the agent migrations are made. This activity is the same as running a software provisioning request.

- Catalina output for destination vRealize Automation: /var/log/vcac/catalina.out. In this file, you see the migrated virtual machines reporting their ping requests here to include version numbers *version*.0-SNAPSHOT. You can tally these together by comparing the EBS topic names, for example, sw-agent-UUID.

- Agent update folder on destination vRealize Automation machine master upgrade log file: /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. You can tail this file to see which upgrade operation is in progress.

- Individual logs available under tenant folders: /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}. Individual nodes are listed here as lot files with failures and in-progress extensions.

- Migrated VMs: /opt/vmware-appdirector/agent/logs/darwin*.log. You can spot check this location which should list the software update requests being received as well as the eventual restart of the agent_bootstrap + software agent.

Set the vRealize Automation PostgreSQL Replication Mode to Synchronous

If you set the PostgreSQL replication mode to asynchronous before upgrade, you can set the PostgreSQL replication mode to synchronous after you upgrade a distributed vRealize Automation environment.

Prerequisites

You have upgraded a distributed vRealize Automation environment.

Procedure

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

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

2   Click **Cluster**.

3   Click **Sync Mode** and wait until the action completes.

4   Verify that all nodes in the Sync State column display `Sync` status.

What to do next

Run Test Connection and Verify Upgraded Endpoints.

Run Test Connection and Verify Upgraded Endpoints

Upgrading from earlier vRealize Automation releases makes changes to certain endpoints in the target environment.

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

The default security setting for upgraded or migrated endpoints is not to accept untrusted certificates.

After upgrading or migrating from an earlier vRealize Automation installation, if you were using untrusted certificates you must perform the following steps for all vSphere and NSX endpoints to enable certificate validation. Otherwise, the endpoint operations fail with certificate errors. For more information, see VMware Knowledge Base articles *Endpoint communication is broken after upgrade to vRA 7.3 (2150230)* at http://kb.vmware.com/kb/2150230 and *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* at http://kb.vmware.com/kb/2108294.

1   After upgrade or migration, log in to the vRealize Automation vSphere agent machine and restart your vSphere agents by using the **Services** tab.

     Migration might not restart all agents, so manually restart them if needed.

2   Wait for at least one ping report to finish. It takes a minute or two for a ping report to finish.

3   When the vSphere agents have started data collection, log in to vRealize Automation as an IaaS administrator.

4   Click **Infrastructure > Endpoints > Endpoints**.

5   Edit a vSphere endpoint and click **Test Connection**.

6   If a certificate prompt appears, click **OK** to accept the certificate.

     If a certificate prompt does not appear, the certificate might currently be correctly stored in a trusted root authority of the Windows machine hosting service for the endpoint, for example as a proxy agent machine or DEM machine.

7   Click **OK** to apply the certificate acceptance and save the endpoint.

8   Repeat this procedure for each vSphere endpoint.

9   Repeat this procedure for each NSX endpoint.

10   Navigate to **Infrastructure > Compute Resources** and right click on your **vCenter Compute** resource and run **Data Collection.**.

If the **Test Connection** action is successful but some data collection or provisioning operations fail, you can install the same certificate on all the agent machines that serve the endpoint and on all DEM machines. Alternatively, you can uninstall the certificate from existing machines and repeat the preceding procedure for the failing endpoint.

Run NSX Network and Security Inventory Data Collection After You Upgrade from vRealize Automation

After you upgrade from vRealize Automation, you must run NSX Network and Security Inventory data collection in the upgraded vRealize Automation environment.

This data collection task is necessary to support the load balancer reconfiguration option in deployments.

Prerequisites

- Run NSX Network and Security Inventory Data Collection Before You Upgrade vRealize Automation.

- Upgrade vRealize Automation.

Procedure

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

Join Replica Appliance to Cluster

After you complete the master vRealize Automation appliance update, each updated replica node is automatically joined to the master node. When a replica node must be separately updated, manually join the replica node to the cluster.

Procedure

1   On the replica node that is not joined to the cluster, log in to the vRealize Automation appliance management interface as root.

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

2   Select **Cluster**.

3   Click **Join Cluster**.

Port Configuration for High-Availability Deployments

After finishing an upgrade in a high-availability deployment, you must configure the load balancer to pass traffic on port 8444 to the vRealize Automation appliance to support remote console features.

For more information, see the *vRealize Automation Load Balancing Configuration Guide* in the vRealize Automation Documentation..

Restore External Workflow Timeout Files

You must reconfigure the vRealize Automation external workflow timeout files because the upgrade process overwrites xmldb files.

Procedure

1   Open the external workflow configuration (xmldb) files on your system from the following directory.

    `\VMware\vCAC\Server\ExternalWorkflows\xmldb\`.

2   Replace the xmldb files with the files that you backed up before migration. If you do not have backup files, reconfigure the external workflow timeout settings.

3   Save your settings.

Restore Changes to Logging in the app.config File

The upgrade process overwrites changes you make to logging in the configuration files. After you finish an upgrade, you must restore any changes you made before the upgrade to the `app.config` file .

Reconfigure the Azure Endpoint Post Upgrade

After upgrade, you must reconfigure your Microsoft Azure endpoint.

Perform this procedure for each Microsoft Azure endpoint.

Prerequisites

■   Successfully upgrade to the target version of vRealize Automation.

■   Log in to the target vRealize Automation console.

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

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

    b   Log in as a IaaS administrator user.

Procedure

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

2   Select a Microsoft Azure endpoint.

3   Click **Edit**.

4   Click **Details**.

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

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

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

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

8   Click **Finish**.

9   Repeat for each Azure endpoint.

Enable Automatic Manager Service Failover After Upgrade

Automatic Manager Service failover is disabled by default when you upgrade vRealize Automation.

Complete these steps to enable automatic Manager Service after upgrade.

Procedure

1   Open a command prompt as root on the vRealize Automation appliance.

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

3   To enable automatic Manager Service failover, run the following command.

    `python ./manager-service-automatic-failover ENABLE`

    To disable automatic failover throughout an IaaS deployment, run the following command.

    `python ./manager-service-automatic-failover DISABLE`

About Automatic Manager Service Failover

You can configure the vRealize Automation IaaS Manager Service to automatically fail over to a backup if the primary Manager Service stops.

Starting in vRealize Automation 7.3, you no longer need to manually start or stop the Manager Service on each Windows server, to control which serves as primary or backup. Automatic Manager Service failover is disabled by default when you upgrade IaaS with the Upgrade Shell Script or using the IaaS Installer executable file.

When automatic failover is enabled, the Manager Service automatically starts on all Manager Service hosts, including backups. The automatic failover feature allows the hosts to transparently monitor each other and fail over when necessary, but the Windows service must be running on all hosts.

Note   You are not required to use automatic failover. You may disable it and continue to manually start and stop the Windows service to control which host serves as primary or backup. If you take the manual failover approach, you must only start the service on one host at a time. With automatic failover disabled, simultaneously running the service on multiple IaaS servers makes vRealize Automation unusable.

Do not attempt to selectively enable or disable automatic failover. Automatic failover must always be synchronized as on or off, across every Manager Service host in an IaaS deployment.

Import DynamicTypes Plug-In

If you are using the DynamicTypes plug-in, and you exported the configuration as a package before the upgrade, you must import the following workflow.

1 Import Dynamic Types Configuration in the target environment.

    a   Log in to the Java Client as administrator.

    b   Select the **Workflows** tab.

    c   Select **Library** > **Dynamic Types** > **Configuration**.

    d   Select the **Import Configuration From Package** workflow and run it.

    e   Click **Configuration package to import**.

    f   Browse to the exported package file and click **Attach file**.

    g   Review the information about the namespaces attached to the package and click **Submit**

2 Select **Inventory** > **Dynamic Types** to verify that the dynamic type namespaces have been imported.

Troubleshooting the vRealize Automation Upgrade

<div style="text-align: right;">9</div>

The upgrade troubleshooting topics provide solutions to problems that you might encounter when upgrading vRealize Automation from 7.1 or later.

This chapter includes the following topics:

- Storages Might Be Delayed After Upgrade

- Work Around Upgrade Problems

- Virtual Appliance Upgrade Fails During the IaaS Prerequisite Check

Automatic Manager Service Failover Does Not Activate

Suggestions for troubleshooting manager-service-automatic-failover command.

Solution

- The manager-service-automatic-failover command fails or displays this message for more than two minutes: `Enabling Manager Service automatic failover mode on node:` `IAAS_MANAGER_SERVICE_NODEID`.

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

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

    b Select **Cluster**.

    c Verify that the Management Agent service is running on all Manager Service hosts.

    d Verify that the last connected time for all IaaS Manager Service nodes is less than 30 seconds.

    If you find any Management Agent connectivity issues, resolve them manually and retry the command to enable the Manager Service automatic failover.

- The manager-service-automatic-failover command fails to enable failover on a Manager Service node. It is safe to rerun the command to fix this.

- Some Manager Service hosts in the IaaS deployment have failover enabled while other hosts do not. All Manager Service hosts in the IaaS deployment must have the feature enabled or it does not work. To correct this issue, do one of the following:

    - Disable failover on all Manager Service nodes and use the manual failover approach instead. Only run failover on one host at a time.

    - If multiple attempts fail to enable the feature on a Manager Service node, stop the Windows VMware vCloud Automation Center Service on this node and set the node startup type to Manual until you resolve the issue.

- Use Python to validate that failover is enabled on each Manager Service node.

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

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

    c Verify that the system returns this message: `Enabling Manager Service automatic failover mode on node:` *IAAS_MANAGER_SERVICE_NODEID* done.

- Validate that failover is enabled on each Manager Service node by inspecting the Manager Service configuration file.

  a   Open a command prompt on a Manager Service node.

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

  c   Verify that the following elements are present in the <appSettings> section.

    - <add key="FailoverModeEnabled" value="True" />

    - <add key="FailoverPingIntervalMilliseconds" value="30000" />

    - <add key="FailoverNodeState" value="active" />

    - <add key="FailoverMaxFailedDatabasePingAttepts" value="5" />

    - <add key="FailoverMaxFailedRepositoryPingAttepts" value="5" />

- Verify that Windows VMware vCloud Automation Center Service status is started and startup type is automatic.

- Use Python to validate that failover is disabled on each Manager Service node.

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

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

  c   Verify that the system returns this message: `Disabling Manager Service automatic failover mode on node: IAAS_MANAGER_SERVICE_NODEID done`.

- Validate that failover is disabled on each Manager Service node by inspecting the Manager Service configuration file.

  a   Open a command prompt on a Manager Service node.

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

  c   Verify that the following element is present in the <appSettings> section.

    - <add key="FailoverModeEnabled" value="False" />

- To create a cold standby Manager Service node, set the node Windows VMware vCloud Automation Center Service status to stopped and startup type to manual.

- For an active Manager Service node, the node Windows VMware vCloud Automation Center Service status must be started and startup type must be automatic.

- The manager-service-automatic-failover command uses the Manager Service node internal id - *IAAS_MANAGER_SERVICE_NODEID*. To find the hostname corresponding to this internal id, run the command `vra-command list-nodes` and look for the Manager Service host with NodeId: *IAAS_MANAGER_SERVICE_NODEID*.

- To locate the Manager Service that the system has automatically elected to be currently active, perform these steps.

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

    b   Run `vra-command list-nodes --components`.
    - If failover is enabled, find the Manager Service node with State: Active.

    - If failover is disabled, find the Manager Service node with State: Started.

Installation or Upgrade Fails with a Load Balancer Timeout Error

A vRealize Automation installation or upgrade for a distributed deployment with a load balancer fails with a 503 service unavailable error.

Problem

The installation or upgrade fails because the load balancer timeout setting does not allow enough time for the task to complete.

Cause

An insufficient load balancer timeout setting might cause failure. You can correct the problem by increasing the load balancer timeout setting to 100 seconds or greater and rerunning the task.

Solution

1   Increase your load balancer timeout value to at least 100 seconds.

2   Rerun the installation or upgrade.

Upgrade Fails for IaaS Website Component

The IaaS upgrade fails and you cannot continue the upgrade.

Problem

The Iaas upgrade fails for the website component. The following error messages appear in the installer log file.

- System.Data.Services.Client.DataServiceQueryException:

    An error occurred while processing this request. --->

    System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>

- Description: An application error

    occurred on the server. The current custom error settings for this application

    prevent the details of the application error from being viewed remotely (for

    security reasons). It could, however, be viewed by browsers running on the

    local server machine.

- Warning: Non-zero return code. Command failed.

- Done Building Project "C:\Program Files

    (x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"

    (InstallRepoModel target(s)) -- FAILED.

The following error messages appear in the repository log file.

- [Error]: [sub-thread-Id="20"

    context="" token=""] Failed to start repository service. Reason:

    System.InvalidOperationException: Configuration section encryptionKey is not

    protected

    at

    DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration

    config)

    at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)

    at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2

    decryptFunc)

    at

    DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object

    sender, ObjectMaterializedEventArgs e)

    at

    System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()

    at

    System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()

    at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)

    at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)

    at

    DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core
    ModelEntities

    coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)

    at

    DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()

    at

    DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String

coreModelConnectionString)

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

Cause

Iaas upgrade fails when the creation date for the `web.config` file is the same as or later than the modified date.

Solution

1   On the IaaS host, log in to Windows.

2   Open the Windows command prompt.

3   Change directories to the vRealize Automation installation folder.

4   Start your preferred text editor with the **Run as Administrator** option.

5   Locate and select the `web.config` file and save the file to change its file modification date.

6   Examine the `web.config` file properties to confirm that the file modification date is later than the creation date.

7   Upgrade IaaS.

Manager Service Fails to Run Due to SSL Validation Errors During Runtime

The manager service fails to run due to SSL validation errors.

Problem

The manager service fails with the following error message in the log:

```
[Info]: Thread-Id="6" — context="" token="" Failed to connect to the core database,
will retry in 00:00:05, error details: A connection was successfully established
with the server, but then an error occurred during the login process. (provider: SSL
Provider, error: 0 — The certificate chain was issued by an authority that is not
trusted.)
```

Cause

During runtime, the manager service fails to run due to SSL validation errors.

Solution

1   Open the `ManagerService.config` configuration file.

2   Update **Encrypt=False** on the following line:

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Log In Fails After Upgrade

You must exit the browser and log in again after an upgrade for sessions that use unsynchronized user accounts.

Problem

After you upgrade vRealize Automation, the system denies access to unsynchronized user accounts at login.

Solution

Exit the browser and relaunch vRealize Automation.

Delete Orphaned Nodes on vRealize Automation

An orphaned node is a duplicate node that is reported on the host but does not exist on the host.

Problem

When you verify that each IaaS and virtual appliance node is in a healthy state, you might discover that a host has one or more orphaned nodes. You must delete all orphaned nodes.

Solution

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

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

2   Select **Cluster**.

3   For each orphaned node in the table, click **Delete**.

Join Cluster Command Appears to Fail After Upgrading a High-Availability Environment

After you click **Join Cluster** in the vRealize Automation appliance management interface on a secondary cluster node, the progress indicator disappears.

Problem

When you use the vRealize Automation appliance management interface after upgrade to join a secondary cluster node to the primary node, the progress indicator disappears and no error or success message appears. This behavior is an intermittent problem.

Cause

The progress indicator disappears because some browsers stop waiting for a response from the server. This behavior does not stop the join cluster process. You can confirm that the join cluster process is successful by viewing the log file at `/var/log/vmware/vcac/vcac-config.log`.

PostgreSQL Database Upgrade Merge Does Not Succeed

The external PostgreSQL database merge with the embedded PostgreSQL database does not succeed.

Problem

If the PostgreSQL database upgrade merge does not succeed, you can perform a manual merge.

Solution

1   Revert the vRealize Automation virtual appliance to the snapshot you made before upgrade.

2   Log in to the vRealize Automation virtual appliance and run this command to allow upgrade to complete if the database merge does not succeed.

    touch /tmp/allow-external-db

    The command does not disable auto merge.

3   On the remote PostgreSQL database host, connect to the PostgreSQL database using the psql tool and run these commands.

    ```
    CREATE EXTENSION IF NOT EXISTS "hstore";
    ```

    ```
    CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
    ```

    ```
    CREATE SCHEMA saas AUTHORIZATION vcac;
    ```

    The user in this command is vcac. If vRealize Automation connects to the external database with a different user, replace vcac in this command with the name of that user.

    ```
    CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
    ```

4   Run upgrade.

    If upgrade is successful, the system works as expected with the external PostgreSQL database. Ensure that the external PostgreSQL database is running properly.

5   Log in to the vRealize Automation virtual appliance and run these commands

    ```
    /etc/bootstrap/postupdate.d/00-20-db-merge-external
    ```

    ```
    /etc/bootstrap/postupdate.d/11-db-merge-external
    ```

Replica vRealize Automation Appliance Fails to Update

Replica vRealize Automation appliance fails to update during master appliance update.

Cause

A replica appliance can fail to update due to connectivity issues or other failures. When this happens, you see a warning message on the master vRealize Automation appliance **Update** tab, highlighting the replica that failed to update.

Solution

1   Revert the replica virtual appliance snapshot or backup to the pre-update state and power it on.

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

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

3   Click **Update > Settings**.

4   Select to download the updates from a VMware repository or CDROM in the Update Repository section.

5   Click **Status**.

6   Click **Check Updates** to verify that an update is accessible.

7   Click **Install Updates**.

8   Click **OK**.

    A message stating that the update is in progress appears.

9   Open the log files to verify that upgrade is progressing successfully.

    ■   `/opt/vmware/var/log/vami/vami.log`

    ■   `/var/log/vmware/horizon/horizon.log`

    If you log out during the upgrade process and log in again before the upgrade is finished, you can continue to follow the progress of the update in the log file. The `updatecli.log` file might display information about the version of vRealize Automation that you are upgrading from. This displayed version changes to the proper version later in the upgrade process.

    The time required for the update to finish varies according to your environment.

10 When the update is finished reboot the virtual appliance.

    a   Click **System**.

    b   Click **Reboot** and confirm your selection.

11 Select **Cluster**.

12 Enter the master vRealize Automation appliance FQDN and click **Join Cluster**.

Backup Copies of .xml Files Cause the System to Time Out

vRealize Automation registers any file with an .xml extension in the \VMware\vCAC\Server\ExternalWorkflows\xmldb\ directory. If this directory contains backup files with an .xml extension, the system runs duplicate workflows that cause the system to time out.

Solution

Workaround: When you back up files in this directory, move the backups to another directory, or change the extension of the backup file name to something other than .xml.

Exclude IaaS Upgrade

You can update the vRealize Automation appliance without upgrading the IaaS components.

Use this procedure when you want to update the vRealize Automation appliance without upgrading the IaaS components. This procedure

- Does not stop IaaS services.

- Skips updating the Management Agents.

- Prevents the automatic update of IaaS components after the vRealize Automation appliance updates.

Procedure

1   Open a secure shell connection to the primary vRealize Automation appliance node.

2   At the command prompt, run this command to create the toggle file:

    touch /tmp/disable-iaas-upgrade

3   Manually stop the IaaS services.

    a   Log in to your IaaS Windows server.

    b   Select **Start > Administrative Tools > Services**.

    c   Stop these services in the following order.

        Note   Do not shut down the IaaS Windows server.

        1   Each VMware vRealize Automation Proxy Agent.

        2   Each VMware DEM worker.

        3   The VMware DEM orchestrator.

        4   The VMware vCloud Automation Center service.

4   Access the primary vRealize Automation appliance management interface and update the primary vRealize Automation appliance.

Unable to Create New Directory in vRealize Automation

Trying to add new directory with the first sync connector fails.

Problem

This issue occurs due to a bad `config-state.json` file located in `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

For information about fixing this issue, see Knowledge Base Article 2145438.

vRealize Automation Replica Virtual Appliance Update Times Out

vRealize Automation replica virtual appliance update times out when you update the master virtual appliance.

Problem

When you update the master virtual appliance, the master vRealize Automation management interface Update tab shows a highlighted replica virtual appliance that has reached the update timeout limit.

Cause

The update times out because of a performance or infrastructure issue.

Solution

1   Check the replica virtual appliance update progress.

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

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

    b   Select **Update > Status** and check the update progress.

       Do one of the following.

       ■   If the update fails, follow the steps in the troubleshooting topic Replica vRealize Automation Appliance Fails to Update.

       ■   If the replica virtual appliance upgrade is in progress, wait until the upgrade finishes and go to step 2.

2   Reboot the virtual appliance.

    a   Click **System**.

    b   Click **Reboot** and confirm your selection.

3   Select **Cluster**.

4   Enter the master vRealize Automation virtual appliance FQDN, and click **Join Cluster**.

Some Virtual Machines Do Not Have a Deployment Created During Upgrade

Virtual machines in the missing state at the time of upgrade do not have a corresponding deployment created in the target environment.

Problem

If a virtual machine is in the missing state in the source environment during upgrade, a corresponding deployment is not created in the target environment. If a virtual machine goes out of the missing state after upgrade, you can import the machine to the target deployment using bulk import.

Certificate Not Trusted Error

When you view the infrastructure Log Viewer page in the vRealize Automation appliance console, you might see an endpoint connection failure report with these words, `Certificate is not trusted`.

Problem

On the vRealize Automation appliance console, select **Infrastructure > Monitoring > Log**. On the Log Viewer page, you might see a report similar to this:

Failed to connect to the endpoint. To validate that a secure connection can be established to this endpoint, go to the vSphere endpoint on the Endpoints page and click the Test Connection button.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Cause

Upgrading from earlier releases of vRealize Automation makes changes to the endpoints from your original environment. After vRealize Automation upgrade, the IaaS administrator must review each upgraded endpoint that uses a secure, https, connection. If an endpoint has a `Certificate is not trusted` error, the endpoint does not work properly.

Solution

1   Log in to the vRealize Automation console as an infrastructure administrator.

2   Select **Infrastructure > Endpoints > Endpoints**.

3   Complete these steps for each endpoint with a secure connection.

   a   Click **Edit**.

   b   Click **Test Connection**.

   c   Review the certificate details and click **OK** if you trust this certificate.

   d   Restart the Windows services for all IaaS Proxy Agents used by this endpoint.

4 Verify that `Certificate is not trusted` errors no longer appear on the infrastructure Log Viewer page.

Installation of Upgrade of vRealize Automation Fails While Applying Prerequisite Fixes

Installing or upgrading vRealize Automation fails and an error message appears in the log file.

Problem

When you install or upgrade vRealize Automation, the procedure fails. This usually happens when a fix applied during install or upgrade is not successful. An error message appears in the log file similar to the following: `Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.`

Cause

The Windows environment has a group policy for PowerShell script execution set to Enabled.

Solution

1 On the Windows host machine, run `gpedit.msc` to open the Local Group Policy Editor.

2 In the left pane under **Computer Configuration**, click the expand button to open **Administrative Templates > Windows Components > Windows PowerShell**.

3 For **Turn on Script Execution**, change the state from `Enabled` to `Not Configured`.

Unable to Update DEM and DEO Components

Unable to update DEM and DEO components while upgrading from vRealize Automation 7.2 to 7.3.x

Problem

After upgrading from vRealize Automation 7.2 to 7.3.x, DEM and DEO components installed on custom path, such as D: drive, are not updated.

See Knowledge Base article 2150517.

Update Fails to Upgrade the Management Agent

An error message about the Management Agent appears when you click **Install Updates** on the vRealize Automation appliance management interface Update Status page.

Problem

Upgrade process is unsuccessful. Message appears: `Unable to upgrade management agent on node x.` Sometimes the message lists more than one node.

Cause

Many conditions can cause this problem. The error message identifies only the node ID of the affected machine. More information is found in the `All.log` file for the Management Agent on the machine where the command fails.

Perform these tasks on the affected nodes according to your situation:

Solution

- If the Management Agent service is not running, start the service and restart upgrade on the virtual appliance.

- If the Management Agent service is running and the Management Agent is upgraded, restart upgrade on the virtual appliance.

- If the Management Agent service is running, but the Management Agent is not upgraded, perform a manual upgrade.

  a In the browser, go to the IaaS Installation page.

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

  b Download and run the Management Agent Installer.

  c Reboot the Management Agent machine.

  d Restart upgrade on the virtual appliance.

Management Agent Upgrade is Unsuccessful

The Management Agent upgrade is unsuccessful during vRealize Automation upgrade.

Problem

If a failover incident has switched the primary and secondary Management Agent host, the upgrade is unsuccessful because the automated upgrade process cannot find the expected host. Perform this procedure on each IaaS node where the Management Agent is not upgraded.

Solution

1 Open the All.log in the Management Agent logs folder, which is located at `C:\Program Files (x86)\VMware\vCAC\Management Agent\Logs\`.

   The location of the installation folder might be different from the default location.

2 Search the log file for a message about an outdated or powered off virtual appliance.

   For example, `INNER EXCEPTION: System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond` *IP_Address*`:5480`

3   Edit the Management Agent configuration file at `C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config` to replace the existing alternativeEndpointaddress value with the URL of the primary virtual appliance endpoint.

The location of the installation folder might be different from the default location.

Example of alternativeEndpointaddress in `VMware.IaaS.Management.Agent.exe.config`.

`<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />`

4   Restart the Management Agent Windows service and check the `All.log` file to verify that is working.

5   Run the upgrade procedure on the primary vRealize Automation appliance.

vRealize Automation Update Fails Because of Default Timeout Settings

You can increase the time setting for update if the default setting for synchronising databases is too short for your environment.

Problem

The timeout setting for the Vcac-Config `SynchronizeDatabases` command is not sufficient for some environments where synchronising databases takes longer than the default value of 3600 seconds.

The `cafeTimeoutInSeconds` and `cafeRequestPageSize` property values in the `Vcac-Config.exe.config` file govern the communication between the API and the `Vcac-config.exe` utility tool. The file is at `IaaS installation location\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config`.

You can override the default timeout value just for the `SynchronizeDatabases` command by supplying a value for these optional parameters.

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

If these parameters are not set in the `Vcac-Config.exe.config` file, the system uses the default timeout value.

Upgrading IaaS in a High Availability Environment Fails

Running the IaaS upgrade process on the primary web server node with load balancing enabled fails. You might see these error messages: "System.Net.WebException: The operation has timed out" or "401 - Unauthorized: Access is denied due to invalid credentials."

Problem

Upgrading IaaS with load balancing enabled can cause an intermittent failure. When this happens, you must run the vRealize Automation upgrade again with load balancing disabled.

Solution

1   Revert your environment to the pre-update snapshots.

2   Open a remote desktop connection to the primary IaaS web server node.

3   Navigate to the Windows hosts file at c:\windows\system32\drivers\etc.

4   Open the hosts file and add this line to bypass the web server load balancer.

    IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

    Example:

    10.10.10.5 vra-iaas-web-lb.domain.com

5   Save the hosts file and retry the vRealize Automation update.

6   When the vRealize Automation update competes, open the hosts file and remove the line you added in step 4.

Storages Might Be Delayed After Upgrade

Storages do not appear under the reservation tab.

If storages do not appear under the reservations tab after your upgrade, a restart of the vcac-server is required on all nodes. It might take up to an hour for storages to appear in the resource section under the reservations tab.

Work Around Upgrade Problems

You can modify the upgrade process to work around upgrade problems.

Solution

When you experience problems upgrading your vRealize Automation environment, use this procedure to modify the upgrade process by selecting one of the available flags.

Procedure

1   Open a secure shell connection to the primary vRealize Automation appliance node.

2   At the command prompt, run this command to create the toggle file:

touch *available_flag*

For example: **touch /tmp/disable-iaas-upgrade**

Table 9-1. Available Flags

Flag	Description
/tmp/disable-iaas-upgrade	- Prevents IaaS upgrade process after the virtual appliance restarts. - Prevents the Management Agent upgrade. - Prevents the automatic prerequisite checks and fixes. - Prevents stopping IaaS services.
/tmp/do-not-upgrade-ma	Prevents the Management Agent upgrade. This flag is suitable when the Management Agent is upgraded manually.
/tmp/skip-prereq-checks	Prevents the automatic prerequisite checks and fixes. This flag is suitable when there is a problem with the automatic prerequisite fixes and the fixes have been applied manually instead.
/tmp/do-not-stop-services	Prevents stopping IaaS services. The upgrade does not stop the IaaS Windows services, such as the Manager Service, DEMs, and agents.
/tmp/do-not-upgrade-servers	Prevents the automatic upgrade of all server IaaS components, such as the database, web site, WAPI, repository, Model Mfrontanager data, and Manager Service. **Note** This flag also prevents enabling the Manager Service automatic failover mode.
/tmp/do-not-upgrade-dems	Prevents DEM upgrade.
/tmp/do-not-upgrade-agents	Prevents IaaS proxy agent upgrade.

3 Complete the tasks for your chosen flag.

Table 9-2. Additional Tasks

Flag	Tasks

/tmp/disable-iaas-upgrade	■ Upgrade the Management Agent manually.
	■ Apply any required IaaS prerequisites manually.
	■ Manually stop the IaaS services.
	    a Log in to your IaaS Windows server.
	    b Select **Start > Administrative Tools > Services**.
	    c Stop these services in the following order.
	
	      Note Do not shut down the IaaS Windows server.
	
	      a Each VMware vRealize Automation Proxy Agent.
	      b Each VMware DEM worker.
	      c The VMware DEM orchestrator.
	      d The VMware vCloud Automation Center service.
	■ Start the IaaS upgrade manually after the virtual appliance upgrade is complete.

/tmp/do-not-upgrade-ma	Upgrade the Management Agent manually.
/tmp/skip-prereq-checks	Apply any required IaaS prerequisites manually.

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

/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

4 Access the primary vRealize Automation appliance management console and update the primary vRealize Automation appliance.

Note Because each flag remains active until it is removed, run this command to remove your chosen flag after upgrade: `rm /flag_path/flag_name`. For example, `rm /tmp/disable-iaas-upgrade`.

Virtual Appliance Upgrade Fails During the IaaS Prerequisite Check

IaaS prerequisite check is unable to validate environments configured with a custom IIS website name. Disabling the automated IaaS upgrade corrects the problem.

Problem

The virtual appliance upgrade fails during the IaaS prerequisite check while running pre-install scripts and post-install scripts.

```
Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can
not find path IIS:\Sites\Default Web Site because it does not exist.
```

When the failure occurs, you see an error message similar to: `Applying automatic fix for <prerequisite check name> prerequisite failed.`

Cause

The IaaS prerequisite checker is unable to validate environments configured with a custom IIS website name. To correct the problem, you must disable the automated IaaS prerequisite checker.

Solution

1 Disable the automated IaaS upgrade prerequisite checks and fixes.

2 Run the vRealize Automation upgrade. See Work Around Upgrade Problems.

3 Follow the upgrade prompts. When the prompts direct you to reboot vRealize Automation, you can use the IaaS installer to search for any unsatisfied IaaS prerequisites and fix them manually.

   Note   Do not restart the appliance until you finish the IaaS prerequisites validation.

4 Use the following steps for every IaaS website node.

   a   Download the IaaS installer. See Download the IaaS Installer to Upgrade IaaS Components After Upgrading the vRealize Automation Appliance.

   b   The first time you initialize the IaaS installer, it generates a new configuration file under the same directory with extension `.exe.config`.

   c   Close the IaaS installer and add the following key in the `<appSettings>` section of the configuration file. The key passes your custom website name to the IaaS prerequisite checker.

   ```
   <add key="PreReqChecker.Default.DefaultWebSite"
   value="custom_web_site_name"/>
   ```

   d   Save the configuration file and rerun the IaaS Installer. Follow the onscreen instructions, until the prerequisite validation is finished. If there were any failed prerequisites, fix them manually.

5   Activate the IaaS automatic upgrade by closing the IaaS installer and rebooting the upgraded vRealize Automation appliance.

Note   If you decide to continue the IaaS upgrade manually using the IaaS Installer, first reboot the upgraded vRealize Automation appliance, wait for all services to become registered. You must upgrade and configure all systems that have IaaS components installed. For more information, see Upgrade the IaaS Components After Upgrading vRealize Automation to the Target Release.