Upgrading from vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1

03 May 2018
vRealize Automation 7.3

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Updated Information

This *Upgrading from vRealize Automation 7.1 or 7.2 to 7.3* is updated with each release of the product or when necessary.

This table provides the update history of *Upgrading from vRealize Automation 7.1 or 7.2 to 7.3*.

Revision	Description
03 MAY 2018	■ Revised Exclude IaaS Upgrade. ■ Added Work Around Upgrade Problems.
15 MAR 2018	Global changes to accommodate upgrade to vRealize Automation 7.3.1.
18 JAN 2018	■ Revised Automatic Manager Service Failover Does Not Activate. ■ Added After Rebooting the Virtual Appliance, Automatic IaaS Upgrade Fails and Displays Pending Reboot Error.
04 DEC 2017	■ Added Empty Deployments Are Seen in vRealize Automation After Upgrade. ■ Revised Prerequisites for Upgrading vRealize Automation.
07 AUG 2017	■ Added Empty Deployments Are Seen in vRealize Automation After Upgrade. ■ Added Restore Access to the Built-In vRealize Orchestrator Control Center. ■ Added Reconfigure the Built-In vRealize Orchestrator to Support High Availability. ■ Revised Prerequisites for Upgrading vRealize Automation. ■ Added Unable to Update DEM and DEO Components. ■ Revised Update Fails to Upgrade the Management Agent
002424-01	■ Made minor editorial updates. ■ Changed title and added information to Run Test Connection and Verify Upgraded Endpoints. ■ Added vRealize Orchestrator upgrade topics. 　■ Upgrading a Stand-Alone vRealize Orchestrator Appliance for vRealize Automation 　■ Upgrade Orchestrator Appliance by Using the Default VMware Repository 　■ Upgrade Orchestrator Appliance by Using an ISO Image 　■ Upgrade Orchestrator Appliance by Using a Specified Repository ■ Added vRealize Orchestrator migration topics. ■ Revised Install the Update on the vRealize Automation Appliance and IaaS Components. ■ Revised Certificate Not Trusted Error. ■ Added Installing or Upgrading vRealize Automation Fails.
002424-00	Initial release.

Upgrading vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2 ,7.3 to 7.3.1

<div style="text-align: right">1</div>

You can upgrade of your current vRealize Automation 7.1 or 7.2 environment to 7.3. You can also upgrade your current vRealize Automation 7.1, 7.2, 7.3 environment to 7.3.1. You use upgrade procedures specific to this version to upgrade your environment.

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

1   vRealize Automation appliance

2   IaaS web server

3   vRealize Orchestrator

You must upgrade all product components to the same version.

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

This chapter includes the following topics:

- Prerequisites for Upgrading vRealize Automation
- Checklist for Upgrading vRealize Automation

Prerequisites for Upgrading vRealize Automation

Before you upgrade vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1, review the following prerequisites.

System Configuration Requirements

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

- Verify that all appliances and servers that are part of your deployment meet the system requirements for the latest version. See the *vRealize Automation Support Matrix* at VMware vRealize Automation Documentation.

- Consult the *VMware Product Interoperability Matrix* on the VMware website for information about compatibility with other VMware products.

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

Hardware Configuration Requirements

Verify that the hardware in your environment is adequate for vRealize Automation 7.3.

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 5.5.x (vCNS) has ended, the VCNS custom properties continue to be valid for NSX purposes. See the VMware Knowledge Base article *End of Availability and End of General Support for VMware vCloud Networking and Security 5.5.x (2144733)* at http://kb.vmware.com/kb/2144733 for more information.

- 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 111 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 4.5 GB on the root partition
  - 4.5 GB on the `/storage/db` partition for the master vRealize Automation appliance
  - 4.5 GB on the root partition for each replica virtual appliance

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

General Prerequisites

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

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

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

- You disable any applications that query vRealize Automation.

- Verify that Microsoft Distributed Transaction Coordinator (MSDTC) is enabled on all vRealize Automation and associated SQL servers. For instructions, see the VMware Knowledge Base article *Various tasks fail after upgrading or migrating to VMware vCloud Automation Center (vCAC) 6.1.x (2089503)* at http://kb.vmware.com/kb/2089503.

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

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

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

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

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

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

Checklist for Upgrading vRealize Automation

When you upgrade your vRealize Automation 7.1, 7.2 environment to 7.3 or your 7.1, 7.2, 7.3 environment to 7.3.1, you update all components in a specific order.

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

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

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

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

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

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

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

Task	Instructions
☐ Run NSX Network and Security Inventory Data Collection Before You Upgrade from vRealize Automation 7.1 or 7.2 to 7.3.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
☐ Download updates to the vRealize Automation appliance.	See Downloading vRealize Automation Appliance Updates.
☐ Set the vRealize Automation PostgreSQL replication mode to asynchronous.	See Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.
☐ 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

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 and apply the latest management pack.

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 the preparatory tasks before you upgrade vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1.

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

This chapter includes the following topics:

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

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

Before you upgrade vRealize Automation 7.1, 7.2 to 7.3.x, you must run NSX Network and Security Inventory data collection in your vRealize Automation 7.1, 7.2 or 7.3 environment.

This data collection is necessary for the load balancer reconfigure action to work in vRealize Automation 7.3 or 7.3.1 for 7.1 and 7.2 deployments.

Procedure

- ◆ Run NSX Network and Security Inventory data collection in your source vRealize Automation environment before you migrate to vRealize Automation 7.3. 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 vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1.

Prerequisites

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

- For each appliance in the source environment, back up all the vRealize Automation appliance configuration files in the following directories.

  - `/etc/vcac/`

  - `/etc/vco/`

  - `/etc/apache2/`

  - `/etc/rabbitmq/`

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

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

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

What to do next

Back Up Your Existing vRealize Automation Environment.

Back Up Your Existing vRealize Automation Environment

Before you upgrade from vRealize Automation 7.1, 7.2, to 7.3 or 7.1, 7.2, 7.3 to 7.3.1, shut down and take a snapshot of each vRealize Automation IaaS server on each Windows node and each vRealize Automation appliance on each Linux node. If the upgrade is unsuccessful, use the snapshot to return to the last known good configuration and attempt another upgrade.

For information about starting vRealize Automation, see *Start Up vRealize Automation* in *Managing vRealize Automation*.

Prerequisites

- Backup Prerequisites for Upgrading vRealize Automation.

- Beginning with vRealize Automation 7.0, the PostgreSQL database is always configured in high-availability mode. Log in to vRealize Automation Appliance Management and click **vRA settings > Database** to locate the current Master node. If the database configuration is listed as an external database, create a manual backup of this external database.

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

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

- Verify that you have taken a snapshot of your system while it is shut down. This is the preferred method of taking a snapshot. See your *vSphere 6.0 Documentation.*

If you cannot shut down your system, take an in-memory snapshot of all the nodes. This is the non-preferred method and should only be used if you cannot take a snapshot while the system is shut down.

- If you modified the `app.config` file, make a backup of that file. See Restore Changes to Logging in the app.config File.

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

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

Procedure

1   Log in to your vSphere client.

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

3   On each machine, click **Shutdown guest** in this order.

    a   IaaS Windows Server machines

    b   vRealize Automation appliance.

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   Power on the system. See Start Up vRealize Automation in *Managing vRealize Automation*.

    If you have a high availability environment, complete these steps to power on your virtual appliances.

    a   Start the master vRealize Automation appliance.

    b   Log in to vRealize Automation Appliance Management, click **Services**, and wait until the licensing-service status is REGISTERED.

    c   Start the remaining vRealize Automation appliances at the same time.

    d   Start the primary Web node and wait for the startup to finish.

    e   Start the primary Manager Service machine and wait for 2 to 5 minutes.

    The actual time depends on your site configuration.

    Note   On secondary machines, do not start or run the Windows service unless you are configured for automatic Manager Service failover.

    f   Start the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation proxy agents.

    Note   You can start these components in any order. You do not need to wait for a component to finish before you start another.

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

    a   Click **Services**.

    b   Verify that each service is REGISTERED.

What to do next

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous.

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous

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

Prerequisites

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

- You are logged in as **root** to vRealize Automation Appliance Management at https://vra-va-hostname.domain.name:5480.

Procedure

1 Click **vRA Settings > Database**.

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

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

What to do next

Downloading vRealize Automation Appliance Updates

Downloading vRealize Automation Appliance Updates

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

For best upgrade performance, use the ISO file method.

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

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

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

Prerequisites

- Back up your existing vRealize Automation environment.

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

Procedure

1   To download the update repository ISO file, go to the vRealize Automation product page at www.vmware.com. Click **vRealize Automation Download Resources** to go to the VMware download page.

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 more information, see the links at the bottom of the VMware download page.

3   Verify that your primary virtual appliance is powered on.

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

5   Go to the management console for your virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

7   Click the **Update** tab.

8   Click **Settings**.

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

10 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   Go to the management console for your virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

3   Click the **Update** tab.

4   Click **Settings**.

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

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

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

7   Click **Save Settings**.

Updating the vRealize Automation Appliance and IaaS Components

4

After you finish the upgrade prerequisites and download the virtual appliance update, you install the update on the vRealize Automation 7.1, 7.2 appliance to upgrade to 7.3 or on the 7.1, 7.2, 7.3 appliance to upgrade to 7.3.1.

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`. In 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 can install the update on the vRealize Automation 7.1 or 7.2 virtual appliance to upgrade vRealize Automation and the IaaS components to 7.3. You can install the update on the vRealize Automation 7.1, 7.2, 7.3 virtual appliance to upgrade vRealize Automation and the IaaS components to 7.3.1.

Do not close the management console while you install the update.

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

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

Prerequisites

- Verify that you selected a download method and downloaded the update. See Downloading vRealize Automation Appliance Updates.

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

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

    - vRealize Automation appliance

    - IaaS Website

    - IaaS Manager Service

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

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

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

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

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

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

    a   Go to the management console for your primary virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

    c   Select **vRA settings > Cluster**.

    d   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.

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

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

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

- ■ If you upgrade the IaaS components manually after you update the vRealize Automation 7.1 or 7.2 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 Open the vRealize Automation appliance management console.

 For a distributed environment, open the management console on the master appliance.

 a Go to the management console for your virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

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

3 Select **vRA Settings > Database** and verify that this appliance is the master vRealize Automation appliance.

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

4 Select **Update > Status**.

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

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

7 Click **Install Updates**.

8   Click **OK**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What to do next

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

1   Enable the load balancer vRealize Automation health checks.

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

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

Upgrading the IaaS Server Components Separately If the Update Process Fails

5

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

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

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

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

3   Run the update process on the vRealize Automation appliance.

4   Update the IaaS components separately using the Upgrade Shell Script or the vRealize Automation 7.3 IaaS installer msi package.

This chapter includes the following topics:

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

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

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

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

Use the upgrade shell script to upgrade the IaaS Components after you update each vRealize Automation 7.1, 7.2 appliance to 7.3 or after you update each vRealize Automation 7.1, 7.2, 7.3 appliance to 7.3.1.

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** on the appliance management console. Verify that each service, except for iaas-service, is REGISTERED.

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

  a   On the Open a browser and navigate to the VMware vRealize Automation IaaS Installation page on the appliance at https://*virtual_appliance_host_FQDN*:5480/installer.

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

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

- Verify that your primary IaaS Website and Model Manager node has JAVA SE Runtime Environment 8, 64 bits, update 161 or later installed. After you install Java, you must set the environment variable, JAVA_HOME, to the new version on each server node.

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

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

  a   Log in to the vRealize Automation appliance management console.

  b   Select **vRA Settings > Cluster**.

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

  d   Verify that the Management Agent version is current.

- Exclude IaaS Upgrade.

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

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

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

Procedure

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

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

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

3   Run the upgrade script.

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

    b   Press Enter.

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

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

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

What to do next

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

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

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

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

You can use this alternative method to upgrade IaaS components after you upgrade the vRealize Automation 7.1, 7.2 appliance to 7.3 or the 7.1, 7.2, 7.3 appliance to 7.3.1.

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

After you upgrade the vRealize Automation appliance to 7.3 or 7.3.1, download the IaaS installer to the machine where the IaaS components to be upgraded are installed.

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

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

Prerequisites

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

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

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

Procedure

1   Open a Web browser.

2   Enter the URL for the Windows installer download page.

For example, **`https://vcac-va-hostname.domain.name:5480/installer`**, where *vcac-va-hostname.domain.name* is the name of the primary (master) vRealize Automation appliance node.

3   Click the **IaaS installer** link.

4   When prompted, save the installer file, setup__*vcac-va-hostname.domain.name*@5480.exe, to the desktop.

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

What to do next

Upgrade the IaaS Components After Upgrading the vRealize Automation Appliance

After you upgrade the vRealize Automation Appliance to 7.3 or 7.3.1, you must upgrade the PostgreSQL database and configure all systems that have IaaS components installed. You can use this procedure for minimal and distributed installations.

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

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

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

1 IaaS Web sites

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

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

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

2 Manager Services

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

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

3 DEM orchestrator and workers

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

4 Agents

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

5 Management Agent

Is updated automatically as part of the upgrade process.

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

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

Prerequisites

- Back up your existing vRealize Automation environment.

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

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

- Verify that your primary IaaS Website, Microsoft SQL database, and Model Manager node has JAVA SE Runtime Environment 8, 64bits, update 161 or later installed. After you install Java, you must set the environment variable, JAVA_HOME , to the new version on each server node.

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

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

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

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

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

  c Choose the appropriate task.

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

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

  d Click **Security**.

  e Select all of the following.

  - **Network DTC Access**

  - **Allow Remote Clients**

  - **Allow Inbound**

  - **Allow Outbound**

  - **Mutual Authentication Required**

  f Click **OK**.

Procedure

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

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

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

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

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

3 Click **Next**.

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

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

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

6   Select **Accept Certificate**.

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

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

8   Click **Next**.

9   Configure the upgrade settings.

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

10   Click **Next**.

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

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

12 Click **Next**.

13 Click **Finish**.

14 Verify that all services restarted.

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

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

17 (Optional) Enable Automatic Manager Service Failover. See *Enable Automatic Manager Service Failover* in *Installing vRealize Automation 7.3*.

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

What to do next

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

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

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

Restore Access to the Built-In vRealize Orchestrator Control Center

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

When you upgrade to vRealize Automation 7.3, you need to perform this procedure to accommodate the new Role-Based Access Control feature. This procedure is written for a high-availability environment.

Prerequisites

Make a snapshot of your vRealize Automation environment.

Procedure

1 Log in to the vRealize Automation appliance management console as root by using the appliance host fully qualified domain name, https://*va-hostname.domain.name*:5480.

2 Select **vRA Settings > Database**.

3 Identify the master and replica nodes.

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

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

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

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

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

7   Open the `sso.properties` file.

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

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

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

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

9   Run this command:

    `vcac-vami vco-service-reconfigure`

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

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

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

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

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

    service vco-server restart

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

    service vco-configurator restart

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

14 When all the services are registered, join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the vRealize Orchestrator configuration. For information, see Reconfigure the Built-In vRealize Orchestrator to Support High Availability.

What to do next

Chapter 6 Upgrading vRealize Orchestrator After Upgrading vRealize Automation.

Upgrading vRealize Orchestrator After Upgrading vRealize Automation

6

You must upgrade your vRealize Orchestrator instance when you upgrade from vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1.

With the release of vRealize Orchestrator 7.3, you have two options for upgrading vRealize Orchestrator when you upgrade to vRealize Automation 7.3 or 7.3.1.

- You can migrate your existing external vRealize Orchestrator server to the embedded vRealize Orchestrator included in vRealize Automation 7.3 or 7.3.1.

- You can upgrade your existing standalone or clustered vRealize Orchestrator server to work with vRealize Automation 7.3 or 7.3.1.

This chapter includes the following topics:

- Migrating an External vRealize Orchestrator Server to vRealize Automation
- Upgrading a Stand-Alone vRealize Orchestrator Appliance for vRealize Automation
- Upgrade a vRealize Orchestrator Appliance Cluster for Use with vRealize Automation 7.3

Migrating an External vRealize Orchestrator Server to vRealize Automation

You can migrate your existing external vRealize Orchestrator server to a vRealize Orchestrator instance embedded in vRealize Automation 7.3 or 7.3.1.

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

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

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

- Improves the operational efficiency.

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

- Multiple tenants in the vRealize Automation environment

- Geographically dispersed environment

- Workload handling

- Use of specific plug-ins, such as older versions of the Site Recovery Manager plug-in

Control Center Differences Between External and Embedded Orchestrator

Some of the menu items that are available in Control Center of an external vRealize Orchestrator are not included in the default Control Center view of an embedded Orchestrator instance.

In Control Center of the embedded Orchestrator server, a few options are hidden by default.

Menu Item	Details
Licensing	The embedded Orchestrator is preconfigured to use vRealize Automation as a license provider.
Export/Import Configuration	The embedded Orchestrator configuration is included in the exported vRealize Automation components.
Configure Database	The embedded Orchestrator uses the database that is used by vRealize Automation.
Customer Experience Improvement Program	You can join the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance management interface. See *The Customer Experience Improvement Program* in *Managing vRealize Automation*.

Another options that are hidden from the default Control Center view are the **Host address** text box and the **UNREGISTER** button on the **Configure Authentication Provider** page.

Note To see the full set of Control Center options in vRealize Orchestrator that is built into vRealize Automation, you must access the advanced Orchestrator Management page at https://*vra-va-hostname.domain.name_or_load_balancer_address*:8283/vco-controlcenter/#/?advanced and click the F5 button on the keyboard to refresh the page.

Migrate an External vRealize Orchestrator to vRealize Automation

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

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

Prerequisites

- Successful migration to vRealize Automation 7.3 or 7.3.1.

- Stop the Orchestrator server service on the external Orchestrator.

- Back up the database, including the database schema, of the external Orchestrator server.

Procedure

1   Export the configuration from the external Orchestrator server.

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

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

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

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

2   Migrate the exported configuration into the embedded Orchestrator instance.

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

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

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

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

    d   Navigate to the `/usr/lib/vco/tools/configuration-cli/bin` directory.

    e   Change the ownership of the exported Orchestrator configuration file.

```
chown vco:vco orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

    f   Import the Orchestrator configuration file to the built-in vRealize Orchestrator server, by running the `vro-configure` script with the `import` command.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --
skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path
orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

3   If the external Orchestrator server from which you want to migrate uses the built-in PostgreSQL database, edit its database configuration files.

a   In the `/var/vmware/vpostgres/current/pgdata/postgresql.conf` file, uncomment the `listen_addresses` line.

b   Set the values of `listen_addresses` to a wildcard (*).

```
listen_addresses ='*'
```

c   Append a line to the `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` file.

```
host all all vra-va-ip-address/32 md5
```

Note   The `pg_hba.conf` file requires using a CIDR prefix format instead on an IP address and a subnet mask.

d   Restart the PostgreSQL server service.

```
service vpostgres restart
```

4 Migrate the external Orchestrator database to the embedded one in vRealize Automation.

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

    b   Navigate to the `/usr/lib/vco/tools/configuration-cli/bin` directory.

    c   Run the following command to migrate the database:

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername
database_user --sourceDbPassword database_user_password
```

Note Enclose passwords that contain special characters in single quotation marks.

The *JDBC_connection_URL* depends on the type of database that you use.

```
PostgreSQL: jdbc:postgresql://host:port/database_name
```

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

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

The default database login information is:

database_name	vmware
database_user	vmware
database_user_password	vmware

5 If you migrated vRealize Automation instead of upgrading it, delete the trusted Single Sign-On certificates from the database of the embedded Orchestrator instance.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore
WHERE id='cakeystore-id';"
```

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

    a   Restart the PostgreSQL server service.

You successfully migrated an external Orchestrator server instance to a vRealize Orchestrator instance embedded in vRealize Automation.

What to do next

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

Configure the Built-In vRealize Orchestrator Server

After you export the configuration of an external Orchestrator server and import it to vRealize Automation 7.3, you must configure the Orchestrator server that is built into vRealize Automation.

Prerequisites

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

Procedure

1   Log in to the vRealize Automation appliance over SSH as `root`.

2   Start the Control Center service and the Orchestrator server service of the built-in vRealize Orchestrator server.

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

3   Log in to Control Center of the built-in Orchestrator server as an **administrator**.

   Note   If you migrate from an external vRealize Orchestrator 7.3 instance, skip to step 5.

4   Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

5   If the external Orchestrator was configured to work in cluster mode, reconfigure the Orchestrator cluster in vRealize Automation.

   a   Go to the advanced **Orchestrator Cluster Management** page, at https://*vra-va-hostname.domain.name_or_load_balancer_address*:8283/vco-controlcenter/#/control-app/ha?remove-nodes.

      Note   If the **Remove** check boxes next the existing nodes in the cluster do not appear, you must refresh the browser page by clicking the F5 button on the keyboard.

   b   Select the check boxes next to the external Orchestrator nodes and click **Remove** to remove them from the cluster.

   c   To exit the advanced cluster management page, delete the `remove-nodes` string from the URL and refresh the browser page by clicking the F5 button on the keyboard.

   d   At the **Validate Configuration** page in Control Center, verify that Orchestrator is configured properly.

6   (Optional) Under the **Package Signing Certificate** tab on the **Certificates** page, generate a new package signing certificate.

7   (Optional) Change the values for **Default tenant** and **Admin group** on the **Configure Authentication Provider** page.

8   Verify that the `vco-server` service appears as REGISTERED under the **Services** tab in the vRealize Automation appliance management console.

9 Select the `vco` services of the external Orchestrator server and click **Unregister**.

What to do next

■ Import any certificates that were trusted in the external Orchestrator server to the trust store of the built-in Orchestrator.

■ Join the vRealize Automation replica nodes to the vRealize Automation cluster to synchronize the Orchestrator configuration.

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

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

■ Restart the `vco-configurator` service on all nodes in the cluster.

■ Update the vRealize Orchestrator endpoint to point to the migrated built-in Orchestrator server.

■ Add the vRealize Automation host and the IaaS host to the inventory of the vRealize Automation plug-in, by running the Add a vRA host and Add the IaaS host of a vRA host workflows.

Upgrading a Stand-Alone vRealize Orchestrator Appliance for vRealize Automation

If you maintain a stand-alone, external instance of vRealize Orchestrator for vRealize Automation, you must upgrade vRealize Orchestrator when you upgrade vRealize Automation from 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1.

Embedded instances of vRealize Orchestrator are upgraded as part of the vRealize Automation appliance upgrade. No additional action is required for an embedded instance.

If you are upgrading a vRealize Orchestrator appliance cluster, see Upgrade a vRealize Orchestrator Appliance Cluster for Use with vRealize Automation 7.3.

Prerequisites

■ Install the Update on the vRealize Automation Appliance and IaaS Components.

■ Unmount all network file systems. See *vSphere Virtual Machine Administration* in the vSphere documentation.

■ Increase the memory of the vSphere Orchestrator appliance to at least 6 GB. See *vSphere Virtual Machine Administration* in the vSphere documentation.

■ Take a snapshot of the vSphere Orchestrator virtual machine. See *vSphere Virtual Machine Administration* in the vSphere documentation.

■ If you use an external database, back up the database.

■ If you use the preconfigured PostgreSQL database in vSphere Orchestrator, back up the database by using the **Export Database** menu in the vSphere Control Center.

Procedure

◆ Use one of the documented methods to upgrade your stand-alone vRealize Orchestrator.

  ■ Upgrade Orchestrator Appliance by Using the Default VMware Repository.

  ■ Upgrade Orchestrator Appliance by Using an ISO Image.

  ■ Upgrade Orchestrator Appliance by Using a Specified Repository.

Upgrade Orchestrator Appliance by Using the Default VMware Repository

You can configure Orchestrator to download the upgrade package from the default VMware repository.

Prerequisites

■ Unmount all network file systems. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ Make sure that the root partition of the Orchestrator Appliance has at least 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.

■ Take a snapshot of the Orchestrator virtual machine. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ If you use an external database, back up the database.

■ If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the **Export Database** menu in Control Center.

■ If you use vSphere as an authentication provider an the Platform Services Controller is external to the vCenter Server, you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On.

■ Import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain. For more information, see *Import a Trusted Certificate Through Control Center* in *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1 Go to the Virtual Appliance Management Interface (VAMI) at https://*orchestrator_server*:5480 and log in as `root`.

2 On the **Update** tab, click **Settings**.

   The radio button next to the **Use Default Repository** option is selected.

3 On the **Status** page, click **Check Updates**.

4 If any updates are available, click **Install Updates**.

5 Accept the VMware End-User License Agreement and confirm that you want to install the update.

6 To complete the update, restart the Orchestrator Appliance.

   a   Log in again to the to the Virtual Appliance Management Interface (VAMI) as `root`.

7 (Optional) On the **Update** tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

8 Log in to Control Center as `root`.

9 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.

   a   On the **Host Settings** page in Control Center, click **CHANGE**.

   b   Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

10 Reconfigure the authentication.

   a   If before the upgrade, the Orchestrator server was configured to use **LDAP** or **SSO (legacy)** as an authentication method, configure **vSphere** or **vRealize Automation** as an authentication provider.

   b   If the authentication is already set to **vSphere** or **vRealize Automation**, unregister the settings and register them again.

You successfully upgraded the Orchestrator Appliance.

What to do next

Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

Upgrade Orchestrator Appliance by Using an ISO Image

You can configure Orchestrator to download the upgrade package from an ISO image file mounted to the CD-ROM drive of the appliance.

Prerequisites

■ Unmount all network file systems. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ Make sure that the root partition of the Orchestrator Appliance has at least 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.

■ Take a snapshot of the Orchestrator virtual machine. For more information, see the *vSphere Virtual Machine Administration* documentation.

■ If you use an external database, back up the database.

- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the **Export Database** menu in Control Center.

- If you use vSphere as an authentication provider an the Platform Services Controller is external to the vCenter Server, you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On.

- Import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain. For more information, see *Import a Trusted Certificate Through Control Center* in *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1   Download the `VMware-vRO-Appliance-version-build_number-updaterepo.iso` archive from the official VMware download site.

2   Connect the CD-ROM drive of the Orchestrator Appliance virtual machine. For more information, see the *vSphere Virtual Machine Administration* documentation.

3   Mount the ISO image file to the CD-ROM drive of the appliance. For more information, see the *vSphere Virtual Machine Administration* documentation.

4   Go to the Virtual Appliance Management Interface (VAMI) at https://*orchestrator_server*:5480 and log in as `root`.

5   On the **Update** tab, click **Settings**.

6   Select the radio button next to the **Use CD-ROM updates** option.

7   Return to the **Status** page.

    The version of the available upgrade is displayed.

8   Click **Install Updates**.

9   Accept the VMware End-User License Agreement and confirm that you want to install the update.

10 To complete the update, restart the Orchestrator Appliance.

    a   Log in again to the to the Virtual Appliance Management Interface (VAMI) as `root`.

11 (Optional) On the **Update** tab, verify that the latest version of the Orchestrator Appliance is successfully installed.

12 Log in to Control Center as `root`.

13 If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.

    a   On the **Host Settings** page in Control Center, click **CHANGE**.

    b   Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance name.

14 Reconfigure the authentication.

a   If before the upgrade, the Orchestrator server was configured to use **LDAP** or **SSO (legacy)** as an authentication method, configure **vSphere** or **vRealize Automation** as an authentication provider.

b   If the authentication is already set to **vSphere** or **vRealize Automation**, unregister the settings and register them again.

You successfully upgraded the Orchestrator Appliance.

What to do next

Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

Upgrade Orchestrator Appliance by Using a Specified Repository

You can configure Orchestrator to use a local repository, on which you uploaded the upgrade archive.

Prerequisites

- Unmount all network file systems. For more information, see the *vSphere Virtual Machine Administration* documentation.

- Increase the memory of the Orchestrator Appliance to at least 6 GB. For more information, see the *vSphere Virtual Machine Administration* documentation.

- Make sure that the root partition of the Orchestrator Appliance has at least 3 GB of available free space. For more information on increasing the size of a disk partition, see KB 1004071: http://kb.vmware.com/kb/1004071.

- Take a snapshot of the Orchestrator virtual machine. For more information, see the *vSphere Virtual Machine Administration* documentation.

- If you use an external database, back up the database.

- If you use the preconfigured in Orchestrator PostgreSQL database, back up the database by using the **Export Database** menu in Control Center.

- If you use vSphere as an authentication provider an the Platform Services Controller is external to the vCenter Server, you must configure Orchestrator to connect to the fully qualified domain name or IP address of the Platform Services Controller instance that contains the vCenter Single Sign-On.

- Import to Orchestrator manually the certificates of all Platform Services Controllers that share the same vCenter Single Sign-On domain. For more information, see *Import a Trusted Certificate Through Control Center* in *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1   Prepare the local repository for upgrades.

    a   Install and configure a local Web server.

    b   Download the `VMware-vRO-Appliance-`*`version-build_number`*`-updaterepo.zip` archive
from the official VMware download site.

    c   Extract the `.ZIP` archive to the local repository.

2   Go to the Virtual Appliance Management Interface (VAMI) at https://*orchestrator_server*:5480 and log
in as **root**.

3   On the **Update** tab, click **Settings**.

4   Select the radio button next to the **Use Specified Repository** option.

5   Enter the URL address of the local repository by pointing to the `Update_Repo` directory.

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

6   If the local repository requires authentication, enter user name and password.

7   Click **Save Settings**.

8   On the **Status** page, click **Check Updates**.

9   If any updates are available, click **Install Updates**.

10   Accept the VMware End-User License Agreement and confirm that you want to install the update.

11   To complete the update, restart the Orchestrator Appliance.

    a   Log in again to the to the Virtual Appliance Management Interface (VAMI) as **root**.

12   (Optional) On the **Update** tab, verify that the latest version of the Orchestrator Appliance is
successfully installed.

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

14   If you plan to create a cluster of Orchestrator instances, reconfigure the hosts settings.

    a   On the **Host Settings** page in Control Center, click **CHANGE**.

    b   Enter the host name of the load balancer server instead of the vRealize Orchestrator appliance
name.

15   Reconfigure the authentication.

    a   If before the upgrade, the Orchestrator server was configured to use **LDAP** or **SSO (legacy)** as
an authentication method, configure **vSphere** or **vRealize Automation** as an authentication
provider.

    b   If the authentication is already set to **vSphere** or **vRealize Automation**, unregister the settings
and register them again.

You successfully upgraded the Orchestrator Appliance.

What to do next

Verify that Orchestrator is configured properly at the **Validate Configuration** page in Control Center.

Upgrade a vRealize Orchestrator Appliance Cluster for Use with vRealize Automation 7.3

If you use a vRealize Orchestrator appliance cluster with vRealize Automation, you must upgrade the Orchestrator appliance cluster to version 7.3 by upgrading a single instance and joining newly installed 7.3 nodes to the upgraded instance.

To upgrade a single instance of vRealize Orchestrator, see Upgrading a Stand-Alone vRealize Orchestrator Appliance for vRealize Automation.

Prerequisites

- Install the Update on the vRealize Automation Appliance and IaaS Components.

- Set up a load balancer to distribute traffic among multiple instances of vRealize Orchestrator. See the vRealize Orchestrator Load Balancing Configuration Guide.

- Take a snapshot of all vRealize Orchestrator server nodes.

- Back up the vRealize Orchestrator shared database.

Procedure

1 Stop the `vco-server` and `vco-configurator` Orchestrator services on all cluster nodes.

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

3 Deploy a new Orchestrator appliance on version 7.3.

   a Configure the new node with the network settings of an existing not upgraded instance that is part of the cluster.

4 Access Control Center of the second node to start the configuration wizard.

   a Navigate to https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter.

   b Log in as **root** with the password you entered during OVA deployment.

5 Select the **Clustered Orchestrator** deployment type.

   By choosing this type, you select to join the node to an existing Orchestrator cluster.

6 In the **Hostname** text box, enter the host name or IP address of the first Orchestrator server instance.

   Note This must be the local IP or host name of the Orchestrator instance, to which you are joining the second node. You must not use the load balancer address.

7   In the **User name** and **Password** text boxes, enter the root credentials of the first Orchestrator server instance.

8   Click **Join**. The Orchestrator instance clones the configuration of the node, to which it joins.

The Orchestrator server service of both nodes restart automatically.

9   Access Control Center of the upgraded Orchestrator cluster through the load balancer address and log in as an **administrator**.

10   On the **Orchestrator Cluster Management** page, make sure that the **Active Configuration Fingerprint** and the **Pending Configuration Fingerprint** strings on all nodes in the cluster match.

Note   You might need to refresh the page several times until the two strings match.

11   Verify that the vRealize Orchestrator cluster is configured properly by opening the **Validate Configuration** page in Control Center.

12   (Optional) Repeat steps 3 through 8 for each additional node in the cluster.

You have successfully upgraded the Orchestrator cluster.

What to do next

Chapter 7 Enable Your Load Balancers.

Enable Your Load Balancers 7

If your deployment uses load balancers, re-enable secondary nodes and health checks.

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 .

Post-Upgrade Tasks

<div style="text-align:right">8</div>

After you upgrade vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2. 7.3 to 7.3.1, perform any required post-upgrade tasks.

This chapter includes the following topics:

- 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 vRealize Automation
- Join Replica Appliance to Cluster
- Port Configuration for High-Availability Deployments
- Reconfigure the Built-In vRealize Orchestrator to Support High Availability
- Restore External Workflow Timeout Files
- Enabling the Connect to Remote Console Action for Consumers
- Restore Changes to Logging in the app.config File
- Enable Automatic Manager Service Failover After Upgrade

Set the vRealize Automation PostgreSQL Replication Mode to Synchronous

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

Prerequisites

- You have upgraded a distributed vRealize Automation environment.
- You are logged in as **root** to the appropriate vRealize Automation Appliance Management at https://vra-va-hostname.domain.name:5480.

Procedure

1 Click **vRA Settings > Database**.

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

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

What to do next

Run Test Connection and Verify Upgraded Endpoints

Upgrading to vRealize Automation 7.3 makes changes to endpoints in the target environment.

After you upgrade to vRealize Automation 7.3, 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 to not accept untrusted certificates.

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

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

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

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

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

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

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

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

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

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

8   Repeat this procedure for each vSphere endpoint.

9   Repeat this procedure for each NSX endpoint.

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

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

After you upgrade from vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1, you must run NSX Network and Security Inventory data collection in the vRealize Automation 7.3 or 7.3.1 environment.

This data collection is necessary for the load balancer reconfigure action to work in vRealize Automation 7.3 or 7.3.1 for 7.1 and 7.2 deployments.

Prerequisites

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

- Successful upgrade to vRealize Automation 7.3 or 7.3.1.

Procedure

◆ Run NSX Network and Security Inventory data collection in your source vRealize Automation environment before you migrate to vRealize Automation 7.3. See *Start Endpoint Data Collection Manually* in *Managing vRealize Automation*.

Join Replica Appliance to Cluster

After you complete the master vRealize Automation appliance update, each updated replica node is automatically joined to the master node. In case a replica node has to be separately updated, use these steps to manually join the replica node to the cluster.

Access the appliance management console of the replica node that is not joined to the cluster and perform the following steps.

Procedure

1   Select **vRA Settings > Cluster**.

2   Click **Join Cluster**.

Port Configuration for High-Availability Deployments

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

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

Reconfigure the Built-In vRealize Orchestrator to Support High Availability

For a high-availability deployment, you must manually rejoin each target replica vRealize Automation appliance to the cluster to enable high-availability support for the embedded vRealize Orchestrator.

Prerequisites

Log in to the target replica vRealize Automation appliance management console.

1 Start a browser and open the target replica vRealize Automation management console using the fully qualified domain name (FQDN) of the target replica virtual appliance: https://*vra-va-hostname.domain.name*:5480.

2 Log in with the user name **root** and the password that you entered when you deployed the target replica vRealize Automation appliance.

Procedure

1 Select **vRA Settings > Cluster**.

2 In the **Leading Cluster Node** text box, enter the FQDN of the target master vRealize Automation appliance.

3 Enter the root password in the **Password** text box.

4 Click **Join Cluster**.

Continue past any certificate warnings. The system restarts services for the cluster.

5 Verify that the services are running.

a On the top tab bar, click **Services**.

b Click **Refresh** to monitor the progress of services startup.

Restore External Workflow Timeout Files

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

Procedure

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

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

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

3 Save your settings.

Enabling the Connect to Remote Console Action for Consumers

The remote console action for consumers is supported for appliances provisioned by vSphere in vRealize Automation.

Edit the blueprint after you have upgraded the release and select the **Connect to Remote Console** action on the **Action** tab.

For more information, see Knowledge Base article 2109706.

Restore Changes to Logging in the app.config File

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

Enable Automatic Manager Service Failover After Upgrade

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

Complete these steps to enable automatic Manager Service after upgrade.

Procedure

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

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

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

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

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

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

About Automatic Manager Service Failover

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

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

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

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

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

Troubleshooting the vRealize Automation Upgrade

9

The upgrade troubleshooting topics provide solutions to problems that you might encounter upgrading vRealize Automation 7.1, 7.2 to 7.3 or 7.1, 7.2, 7.3 to 7.3.1.

This chapter includes the following topics:

- Automatic Manager Service Failover Does Not Activate

- Installation or Upgrade Fails with a Load Balancer Timeout Error

- Upgrade Fails for IaaS Website Component

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

- Log In Fails After Upgrade

- Delete Orphaned Nodes on vRealize Automation

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

- PostgreSQL Database Upgrade Merge Does Not Succeed

- Replica vRealize Automation Appliance Fails to Update

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

- Exclude IaaS Upgrade

- Unable to Create New Directory in vRealize Automation

- vRealize Automation Replica Virtual Appliance Update Times Out

- Some Virtual Machines Do Not Have a Deployment Created During Upgrade

- Certificate Not Trusted Error

- Installing or Upgrading vRealize Automation Fails

- Unable to Update DEM and DEO Components

- Update Fails to Upgrade the Management Agent

- Management Agent Upgrade is Unsuccessful

- Empty Deployments Are Seen in vRealize Automation After Upgrade

- After Rebooting the Virtual Appliance, Automatic IaaS Upgrade Fails and Displays Pending Reboot Error

- [IaaS Repository Application Fails](#)

- [Upgrading IaaS in a High Availability Environment Fails](#)

- [Work Around Upgrade Problems](#)

Automatic Manager Service Failover Does Not Activate

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

Solution

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

  a   Log in to vRealize Automation appliance management at https://*va-hostname.domain.name*:5480 with the user name **host** and the password you entered when you deployed the appliance.

  b   Select **vRA Settings > Cluster**.

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

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

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

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

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

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

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

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

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

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

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

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

  a   Open a command prompt on a Manager Service node.

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

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

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

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

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

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

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

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

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

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

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

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

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

  a   Open a command prompt on a Manager Service node.

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

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

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

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

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

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

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

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

b   Run `vra-command list-nodes --components`.

- If failover is enabled, find the Manager Service node with State: Active.

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

Installation or Upgrade Fails with a Load Balancer Timeout Error

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

Problem

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

Cause

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

Solution

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

2   Rerun the installation or upgrade.

Upgrade Fails for IaaS Website Component

The IaaS upgrade fails and you cannot continue the upgrade.

Problem

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

- System.Data.Services.Client.DataServiceQueryException:

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

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

- Description: An application error

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

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

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

  local server machine.

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

- Done Building Project "C:\Program Files

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

  (InstallRepoModel target(s)) -- FAILED.

The following error messages appear in the repository log file.

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

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

  System.InvalidOperationException: Configuration section encryptionKey is not

  protected

  at

  DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration

  config)

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

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

  decryptFunc)

  at

  DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object

  sender, ObjectMaterializedEventArgs e)

  at

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

  at

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

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

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

  at

  DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(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   Log in to the IaaS website component server as administrator.

2   Change directories to the vRealize Automation installation folder.

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

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

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

6   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   Go to the management console for your virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

3   Select **vRA settings > Cluster**.

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

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

After you click **Join Cluster** in the management console on a secondary cluster node, the progress indicator disappears.

Problem

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

Cause

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

PostgreSQL Database Upgrade Merge Does Not Succeed

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

Problem

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

Solution

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

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

    touch /tmp/allow-external-db

    The command does not disable auto merge.

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

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

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

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

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

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

4   Run upgrade.

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

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

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

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

Replica vRealize Automation Appliance Fails to Update

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

Cause

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

Solution

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

2   Open the vRealize Automation appliance management console on the replica appliance.

   a   Go to the management console for your virtual appliance by using its fully qualified domain name, https://*va-hostname.domain.name*:5480.

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

3   Click **Update > Settings**.

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

5   Click **Status**.

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

7   Click **Install Updates**.

8   Click **OK**.

   A message stating that the update is in progress appears.

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

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

   ▪   `/var/log/vmware/horizon/horizon.log`

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

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

10   When the update is finished reboot the virtual appliance.

   a   Click **System**.

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

11   Select **vRA Settings > Cluster**.

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

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

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

Solution

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

Exclude IaaS Upgrade

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

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

- Does not stop IaaS services.

- Skips updating the Management Agents.

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

Procedure

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

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

    touch /tmp/disable-iaas-upgrade

3 Manually stop the IaaS services.

    a Log in to your IaaS Windows server.

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

    c Stop these services in the following order.

        Note Do not shut down the IaaS Windows server.

        1 Each VMware vRealize Automation Proxy Agent.

        2 Each VMware DEM worker.

        3 The VMware DEM orchestrator.

        4 The VMware vCloud Automation Center service.

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

Unable to Create New Directory in vRealize Automation

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

Problem

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

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

vRealize Automation Replica Virtual Appliance Update Times Out

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

Problem

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

Cause

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

Solution

1   Check the replica virtual appliance update progress.

   a   Go to the management console for your replica virtual appliance by using its fully qualified domain name (FQDN), https://*va-hostname.domain.name*:5480.

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

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

   Do one of the following.

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

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

2   Reboot the virtual appliance.

   a   Click **System**.

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

3   Select **vRA Settings > Cluster**.

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

Some Virtual Machines Do Not Have a Deployment Created During Upgrade

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

Problem

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

Certificate Not Trusted Error

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

Problem

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

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

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

Cause

Upgrading to vRealize Automation 7.3 makes changes to the endpoints from your original environment. For environments recently upgraded to vRealize Automation 7.3, the IaaS administrator must review each existing endpoint that uses a secure, https, connection. If an endpoint has a `Certificate is not trusted` error, the endpoint does not work properly.

Solution

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

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

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

   a   Click **Edit**.

   b   Click **Test Connection**.

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

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

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

Installing or Upgrading vRealize Automation Fails

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

Problem

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

Cause

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

Solution

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

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

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

Unable to Update DEM and DEO Components

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

Problem

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

See Knowledge Base article 2150517.

Update Fails to Upgrade the Management Agent

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

Problem

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

Cause

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

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

Solution

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

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

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

    a   Open a browser and navigate to the vRealize Automation IaaS installation page on thevRealize Automation appliance at `https://` `va-hostname.domain.name`:5480/install.

    b   Download and run the Management Agent Installer.

    c   Reboot the Management Agent machine.

    d   Restart upgrade on the virtual appliance.

Management Agent Upgrade is Unsuccessful

The Management Agent upgrade is unsuccessful while upgrading from vRealize Automation to the latest version.

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.

Empty Deployments Are Seen in vRealize Automation After Upgrade

Post provisioning actions appear to complete successfully but no change actually takes place.

Problem

Upgrade process causes some virtual machines to become assigned to the wrong deployment. For information, see Knowledge Base article 2151400.

After Rebooting the Virtual Appliance, Automatic IaaS Upgrade Fails and Displays Pending Reboot Error

After you reboot the virtual appliance, the automatic IaaS upgrade command `upgrade-server` fails and a `Pending reboot` error appears.

Problem

An anti-virus program running on the virtual appliance causes this problem. For information, see Knowledge Base article 52211.

IaaS Repository Application Fails

The presence of Microsoft Monitoring Agent service can cause the IaaS repository application to fail.

Problem

IaaS repository fails and a "System.Web.Http.dll" version 4.0.0.0 error appears in the Repository.log. For information, see Knowledge Base article 52444.

Upgrading IaaS in a High Availability Environment Fails

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

Problem

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

Solution

1   Revert your environment to the pre-update snapshots.

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

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

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

   IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

   Example:

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

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

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

Work Around Upgrade Problems

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

Solution

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

   Procedure

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

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

touch *available_flag*

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

Table 9-1. Available Flags

Flag	Description
/tmp/disable-iaas-upgrade	- Prevents IaaS upgrade process after the virtual appliance restarts. - Prevents the Management Agent upgrade. - Prevents the automatic prerequisite checks and fixes. - Prevents stopping IaaS services.
/tmp/do-not-upgrade-ma	Prevents the Management Agent upgrade. This flag is suitable when the Management Agent is upgraded manually.
/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`.