vmware®

vRealize Automation 7.4 Release Notes

Check regularly for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- What's New
- Internationalization
- System Requirements
- Documentation
- Using vRealize Code Stream
- Resolved Issues
- Known Issues

What's New

The vRealize Automation 7.4 release includes resolved issues and the following new capabilities.

Custom Request Forms Designer

vRealize Automation 7.4 is greatly optimized for service architects, thanks to the new Custom Request Forms Designer that provides a consistent experience in designing infrastructure and application catalog items. It facilitates creation of generic blueprints with a simplified yet rich presentation layer applicable to different lines on business. The out-of-the-box Custom Request form removes the need for wrapping infrastructure and PaaS blueprints into XaaS blueprints, which reduces blueprint sprawl and lowers the cost of ownership.

When leveraging Custom Forms, designer blueprint architects are able to apply the following logic to the blueprint request form:

- Drag-and-drop controls and custom properties on the canvas
- Leverage blueprint schema – blueprint properties, custom properties, and profiles
- Use generated forms
- Save, clear, and revert customized forms
- Dynamically show or hide fields based on custom conditional logic
- Auto-fill and dynamically populate input values based on external and internal logic

- Use internal dependencies and external call outs with vRealize Orchestrator
- Apply constraints to input values
- Apply custom validation using regular expressions
- Apply custom help text and error messages
- Choose vRealize Orchestrator inventory objects
- Support for complex types like disk volumes and vRealize Orchestrator composite types
- Use advanced formatting and apply custom CSS to the blueprint request form
- Automatic form validation of blueprint definition during design time
- Export and import of customized form through GUI and CLI

For information, see [Providing Service Blueprints to Users](#).

Deploy from OVF

- New provisioning option to deploy vSphere blueprints from an OVF or OVA

- Specify URL to the OVF location with authentication and proxy options available

- Support for advanced configuration options in the form of custom properties specific to the OVF

- Support for parameterization with the image component profile

For information, see [Configuring a Blueprint to Provision from an OVF](#).

Improved Integration with vRealize Operations for Workload Placement

We have enhanced our integration with vRealize Operations to optimize the placement of workloads at deployment time. Workload placement now takes into account storage reservation policies configured in vRealize Automation.

For information, see [Effect of vRealize Automation Storage Reservation Policies](#)

Install, Upgrade, and Migrate Improvements

- Certificate Management consolidated on a common page in vRealize Automation Appliance Management

- IaaS service status in vRealize Automation Appliance Management under Cluster tab

- Support for vRealize Automation host renaming

- Support for vra-command implementations in Python

- Faster log rotation and added rotation for RabbitMQ and HealthBroker services

- Log file formats updated to show local and UTC timestamps

- LogInsight agent extended configuration is added to vRealize Automation Appliance Management

- Enable vRealize Orchestrator configurator start, stop, and reset options through vRealize

Automation Appliance Management instead of CLI disabled by default

- vRealize Automation Appliance Management tab for Software Agents upgrade

- Automated migration for embedded vRealize Orchestrator

- Clean up migration package after migration is complete

- Disable editing default tenant or administrator fields

For more information, see Installing or Upgrading vRealize Automation.

vRealize Automation Patch Management

Added support for cumulative patches.

- Tracking of delivered and deployed hotpatches

- Warning that patches need to be installed on the additional nodes in a clustered environment

- Retry on failed installation

- Rollback to the previous patch

- Patch history available

For more information, see Access Patch Management.

Just-in-Time User Provisioning

We provided Just-in-Time (JIT) provisioning capability in vRealize Automation. After configuring JIT, users are auto-created upon first login and user attributes are synced upon subsequent logins. In addition, we provided vIDM dynamic group membership. The vIDM dynamic group is exposed to vRealize Automation and advanced group membership can be used to create, update, or delete custom group membership. Custom groups can also be migrated. The API for this feature is provided as well.

For information, see Configure Just-in-Time User Provisioning.

Improved Handling of Stuck Requests

- Cancel requests that are stuck in an in-progress state by means of API or CloudClient and clean up provisioned resources associated with the canceled request

- New filter on Requests tab to hide failed and canceled requests

For information, see vRealize CloudClient 4.5.

Security

- Message board portlet security enhancements

- Introducing a whitelist for URLs that can be displayed on the message board
- TLS 1.2 protocol is now the default protocol for secure communication

For information, see [Create a Message Board Portlet URL Whitelist](#).

Multitenancy in VMware vRealize Orchestrator

Multitenant architecture is introduced in vRealize Orchestrator 7.4.

For information, see [Multitenancy in VMware vRealize Orchestrator](#).

Support for Microsoft NT LAN Manager (NTLM) authentication using the embedded vIDM instance is deprecated in vRealize Automation 7.4

Note: This release includes all of the issues that were fixed in vRealize Automation 7.3.1. For information, see [vRealize Automation 7.3.1 Release Notes](#).

Internationalization

vRealize Automation 7.4 is available in the following languages:

- English
- French
- German
- Spanish
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese
- Italian
- Russian
- Dutch
- Brazilian Portuguese

For more information about product language support, see the [VMware Product Globalization Guide](#).

System Requirements

For information about supported host operating systems, databases, and Web servers, see the [vRealize Automation Support Matrix](#).

Documentation

For vRealize Automation 7.4 documentation, see [VMware vRealize Automation](#) at VMware Docs.

Installation

For prerequisites and installation instructions, see Installing vRealize Automation at VMware Docs.

Upgrade

For general guidance, see Upgrading vRealize Automation at VMware Docs.

Before you upgrade from vRealize Automation 6.2.x

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

Using vRealize Code Stream

To use vRealize Code Stream in your vRealize Automation environment, you must have a vRealize Code Stream license.

You can enter the license in the vRealize Automation Installation Wizard, or in the vRealize Automation Appliance Management Interface.

For more information, see

- vRealize Code Stream Information Center. See vRealize Code Stream Installation and Apply a vRealize Code Stream License to an Appliance
- vRealize Automation Information Center. See Licensing vRealize Code Stream.

Resolved Issues

- **New Resource Actions cannot map external parameters including vCloud:VM and VC:VirtualMachine**
  The vCloud:VM input parameter of the custom action is greyed out and cannot be selected as input of the scripting action in XaaS form editor.

- **A Distributed Execution Manager (DEM) or Distributed Execution Manager Orchestrator (DEO) does not update when you upgrade to vRealize Automation 7.3.x.**
  The DEM or DEO IaaS component must be installed in the default location at c:\program files (x86)\vmware\vcac when you upgrade to vRealize Automation 7.3.x. If these components are not installed in the default location, they do not update during upgrade.

- **The download links on the Guest and Software Agent Installers page for the Java Runtime Environment for Linux are incorrect**
  These links appear in the Linux Software Installers section.

  - vmware-jre-1.8.0_121-fcs.i586.rpm
  - vmware-jre-1.8.0_121-fcs.x86_64.rpm

  When you click one of these links, a new page opens and displays an HTTP Status 404 – Not Found error.

Workaround: To download these RPM files:

1. Replace the file name in the URL that appears in the browser address field after you click the link.

- Replace vmware-jre-1.8.0_121-fcs.i586.rpm with vmware-jre-1.8.0_121-fcs_b31.i586.rpm.
- Replace vmware-jre-1.8.0_121-fcs.x86_64.rpm with vmware-jre-1.8.0_121-fcs_b31.x86_64.rpm.

For example:

- https://va-hostname.domain.name/software/download/vmware-jre-1.8.0_121-fcs_b31.x86_64.rpm
- https://va-hostname.domain.name/software/download/vmware-jre-1.8.0_121-fcs_b31.i586.rpm

2. Press Enter.

Even though the error message remains in the browser, the file downloads successfully.

- **Unable to add a NAT port forwarding rule to a deployed on-demand NAT network associated with a third-party IPAM provider**
  When you add a NAT port forwarding rule by using the Change NAT Rules post-provisioning action to a deployed on-demand NAT network associated with a third-party IPAM provider, the drop-down menu for the **Component** field does not display any data and cannot accept new data. This prevents you from adding a new rule.

- **Define Virtual Server Distribution Settings procedure contains unsupported HTTPS traffic pattern**
  The Define Virtual Server Distribution Settings procedure contains the following substep.

  Select SSL Session ID to support one of the following supported HTTPS traffic patterns:

  - SSL Passthrough - Client -> HTTPS-> LB (SSL passthrough) -> HTTPS -> server
  - Client - HTTP-> LB -> HTTP -> servers

  If you select the Client - HTTP pattern, the system uses the SSL Passtrough - Client traffic pattern instead. vRealize Automation does not support the Client - HTTP traffic pattern.

- **The Change NAT Rules post-provisioning action fails for a blueprint imported from YAML**
  When invoked on a deployment, the Change NAT Rules post-provisioning action fails with the following error: Failed to invoke deployment update request [{Could not determine current component state for nat1}]. This happens when the blueprint associated with the deployment is imported from a YAML file containing an on-demand NAT network that has non-identical values in its name and ID fields.

- **Endpoints are missing after upgrade to vRealize Automation 7.3 or 7.3.1 if the endpoints have specific vRealize Orchestrator properties added**
  A vRealize Orchestrator endpoint-specific custom property causes endpoint upgrade to fail.

- **Advanced Services option was removed from the Administration menu**
  You can no longer configure the default workflow folder for a tenant via**Administration > Advanced Services > Default vRO Folder**. This option was removed.

Known Issues

The known issues are grouped as follows.

- [Installation](#)
- [Upgrade](#)
- [Configuration and Provisioning](#)
- [Previous Known Issues](#)

Installation

- **New** **Java update 1.8, versions u192, u201, and u202, are incompatible with 7.4 installations.**
  The latest Java update 1.8, versions u192, u201, and u202, can cause problems with the IaaS Database installation if the automatic prerequisite fixes have not been applied.

  Workaround: Use Java version 1.8 u191. Alternatively, you can install 7.4 with the automatic prerequisite fixes enabled to install the older Java version 1.8 u191 on the IaaS machines. After the installation completes, the newer Java version 1.8 u201 or u202 can be installed manually.

Upgrade

- **When upgrading vRealize Automation appliances you might experience failures related to duplicates in the database for the vRealize Orchestrator service**
  The failure shown in the UI will be similar to the following:

  - Failed to install updates (Error while running post-install scripts)
  - VA-check: finished
  - Pre-install: finished
  - Post-install: failed
  - Update failed (code 0-2). Check logs in /opt/vmware/var/log/vami or retry update later.

  The errors listed in /var/log/bootstrap/postupdate.log will include:

  Resolve duplicates by deleting unnecessary items.

  Duplicate entries found in the Orchestrator database:

  Resource element duplicates:

  - 1 item with ID '<UUID>' and name 'ko.properties'
  - 1 item with ID '<UUID>' and name 'fr_FR.properties'
  - 1 item with ID '<UUID>' and name 'zh_CN.properties'

  (and many more)

  Workaround: Apply the workaround before you upgrade to 7.4. See Knowledge Base

article <u>54982</u>.

- **NEW Custom updates in setenv.sh file for vRO are overidden after upgrading.**
  Post upgrade, manually update the values as needed post upgrade and restart the VCO server to apply the changes.

- **NEW vRA portal is down (services are unavailable) after upgrade or after changing the SSO admin password**
  If the user has configured a custom vRO authentication provider in the vRO Control Center, this value gets overridden by the default value (vsphere.local\vcoadmins) after upgrade or after changing the SSO admin password.

  Workaround: See Knowledge Base article <u>56627</u>.

Configuration and Provisioning

- **401 Unauthorized error received**
  The vRealize Automation API calls the VMware Identity Manager (vIDM) API. Because vIDM does not support API authentication for an external/third-party Identity Provider (IDP) and third-party IDP, authentication fails when the third-party IDP is used. However, third-party IDP is a prerequisite for enabling and configuring the Just-in-Time (JIT) user provisioning capability of vIDM. So JIT users cannot authenticate using the vRealize Automation API.

  Workaround: API authentication using the OAuth2 password grant type requires one of the following password authentication methods to exist in vIDM:

  - Connector password auth
  - Connector (outbound) password auth
  - Local user password
  - Acc Password

  Even when a third-party IDP is configured for authentication, one of the passwords must exist. To work around this problem, local users can authenticate using the vRealize Automation API.

- **Resume request fails**
  Resume request can fail in these situations:

  1. Resume request fails on a component request where a machine is successfully allocated but the provisioning fails. This happens when the system attempts to reprovision a machine using allocation information that is no longer valid.
  2. Resume request on a nested blueprint fails. Resume request operation fails to initialize the inner blueprint's requests correctly when recreating component requests.

  Workaround: None

- **A XaaS field that is bound to _asd.requestInfo_~requestedBy or _asd.requestInfo_~requestedFor is incorrectly evaluated when XaaS is in a component blueprint**
  A XaaS field with a value constraint that is bound to _asd.requestInfo_, requestedFor, or requestedBy evaluates to the last person who edited and saved the XaaS blueprint.

Workaround:

1. Remove the value constraint from the bound XaaS field.
2. Set a default value on this field and bind it to
   asd.requestInfo~requestedBy~principalId.
3. Delete and re-drag the XaaS component to the composite blueprint canvas.
4. Save the composite blueprint.

- **When you cancel a catalog item request immediately after you submit it, the process appears stuck in the CANCELLING state**
  System does not call the request completion event which could lead to the request being stuck in the CANCELLING state.

  Workaround: Do not cancel a catalog request immediately after submitting. Wait until process moves to IN-PROGRESS state.

- **Editing a Connector Auth Adapter can require login**
  Administrators can use the vRealize Automation console to configure Auth Adapters for Connectors corresponding to a directory within 30 minutes of logging in to the console. If an administrator attempts to perform this configuration after 30 minutes, a login page is displayed and authentication is required.

  Workaround: Log in to the console again with administrator credentials.

- **You are asked to log in again to vRealize Automation Appliance Management after you have logged in successfully**
  After you click Patch Management in vRealize Automation Appliance Management, you are asked enter your credentials again.

  Workaround: Re-authenticate as root user to use the patch management page.

- **When the primary domain controller is unavailable, the login is very slow or fails**
  When an attempt to contact the primary domain controller fails, vIDM contacts the secondary domain controller. Because vIDM always contacts the primary domain controller before contacting the secondary domain controller, there is a delay in processing the login requests. This causes the requests to pile up and slow down the system.

  Workaround: See Knowledge Base article 52840.

- **After a successful migration from vRealize Automation 7.3 to 7.4, you receive a failure message for some operations on Azure resources**
  After a successful migration from vRealize Automation 7.3 to 7.4, some operations, such as restart, intermittently fail on migrated Azure resources. These failures are reported in vRealize Automation even though the vRealize Orchestrator workflow succeeds.

  Workaround: Open a new command prompt and run these commands and make the requested edits to increase the timeout values in o11n-gateway and shindig-ui properties and restart the vcac-server.

  1. # cd /var/lib/vcac/server/webapps/vcac/WEB-INF/classes/

  2. # cp shindig.properties shindig.properties.`date +%m%d%Y`

3. # vi shindig.properties

4. edit > shindig.http.client.read-timeout-ms=150000

5. # cd /usr/lib/vcac/server/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root

6. # cp o11n-gateway-service-context.xml o11n-gateway-service-context.xml.`date +%m%d%Y`

7. # vi o11n-gateway-service-context.xml

8 edit > to 150000

9. # service vcac-server restart

- **The vRealize Automation health service shows multiple errors when one or more virtual appliances are unavailable**
  When one or more virtual appliances are unavailable, the health service shows errors. Some errors can obscure additional errors that are occurring.

  Workaround:Restore the failed node or remove the node from the cluster to reveal any hidden errors.

- **Clicking the Start, Stop, or Restart buttons under the Xenon tab on vRealize Automation Appliance Management does not affect the service**
  In a clustered environment, the start, stop, or restart operations under the Xenon tab on vRealize Automation Appliance Management do not affect the service if executed from a replica node.

  Workaround: Xenon service operations should only be executed on the master node.

- **When you start a browser and open vRealize Automation Appliance Management, an error message about a self-signed certificate appears and you cannot proceed**
  Browsers with HTTP Strict Transport Security (HSTS) enabled prevent access to sites with a self-signed certificate.

  Workaround: See Knowledge Base article 53533.

- **Manager Service automatic failover mode is enabled after running the automatic IaaS upgrade to 7.4**
  If you upgrade or migrate to vRealize Automation 7.4 from 7.3 or 7.3.1 and have deliberately disabled automatic failover before upgrade or migration, the feature is enabled during the automatic IaaS upgrade to 7.4.

  To disable Manager Service automatic failover mode, complete one of these tasks.

    - Disable automatic Manager Service failover
      For information, seeEnable Automatic Manager Service Failover in Installing vRealize Automation.

    - Upgrade IaaS manually using the legacy installer

For information, see[Download the IaaS Installer to Upgrade IaaS Components](#)in Upgrading vRealize Automation 6.2.5 to 7.4.

- **The post provisioning operation Manage Public IP Address for an Azure virtual machine times out**
  The time required to fetch the Azure virtual machine's current and available public address through vRealize Orchestrator is too long. The process times out in vRealize Automation with this error message: "The connection to vCenter Orchestrator Server time out."

  Workaround:

  Complete this procedure to increase the timeout setting in vRealize Automation.

  1. On each vRealize Automation appliance host, open a command prompt using SSH and log in as root.
  2. Run this command to stop vRealize Automation services on all nodes:service vcac-server stop
  3. Change directories to /etc/vcac/ and open the vcac.properties file with a text editor.
  4. Increase the timeout value for the vco.socket.timeout.millis property to 300000. For example, vco.socket.timeout.millis= 300000. The setting is in milliseconds.
  5. Save and close the vcac.properties file.
  6. Change directories to /var/lib/vcac/server/webapps/vcac/WEB-INF/classes/.
  7. Run this command to back up the shindig.properties file:cp shindig.properties shindig.properties.bak
  8. Open the shindig.properties file with a text editor and locate the line in the file that looks similar to shindig.http.client.read-timeout-ms=70000.
  9. Increase the shindig.http.client.read-timeout-ms value to 300000. For example, shindig.http.client.read-timeout-ms=300000.
  10. Save and close the shindig.properties file.
  11. Change directories to /etc/vcac/ and open the setenv-user file with a text editor.
  12. Add this line to the file: VCAC_OPTS="$VCAC_OPTS -Dclient.system.socket.timeout=300000"
  13. Save and close the setenv-user file.
  14. Run this command to start vRealize Automation services on all nodes:service vcac-server start

- **In a clustered vRealize Automation environment, replica appliances can achieve 100% CPU utilization**
  In a clustered vRealize Automation environment, replica appliances can achieve 100% CPU utilization due to multiple socat processes.

  Workaround: See Knowledge Base article [54143](#).

- **Sync of active directory fails**
  1. AD has more than 200 K users and 60 K groups.
  2. Top level domain, like abc.com, is used to sync instead of sub-domains, like subdomain1.abc.com.

  Symptom:

  connector (located in /var/log/vmware/horizon folder of cafe) log throws error:

2018-03-23 18:01:22,122 ERROR (SimpleAsyncTaskExecutor-168) [3259@JNJ;local@JNJ;127.0.0.1] com.vmware.horizon.directory.ldap.LdapConnector - Problem reading from LDAP directory: javax.naming.OperationNotSupportedException: [LDAP: error code 12 - 00002040: SvcErr: DSID-03140395, problem 5010 (UNAVAIL_EXTENSION), data 0

1. Sync of AD has to performed for each individual OU allowing a maximum of 120 K users and 40 K groups in one OU.
2. Safeguards have to be ignored from Sync Settings > Safeguards page.

Previous Known Issues

To view a list of previous known issues, click[here](#).