Installation and Configuration

vRealize Code Stream 2.0

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

Installation and Configuration 5

1 vRealize Code Stream Installation 7
- Preparing for Installation 8
- Using vRealize Code Stream Installation Checklist 11
- Installation Worksheet 12
- Installing vRealize Automation with the Installation Wizard 12
- Installing vRealize Automation through the Standard Interfaces 14
- Apply a vRealize Code Stream License to an Appliance 19
- Set Up the Artifactory Server Password 19

2 Configuring Components 21
- Managing Users 21
- Configure a Tenant to a User in the Artifactory Server 24
- Configure an External Disk Partition for the Artifactory Server 25
- Publish a Service Blueprint as a Catalog Item 25

3 Registering Components 27
- Register an Artifactory Server for Artifact Management 27
- Registering Plug-In Instances and Endpoints for a Release Pipeline 28

4 Troubleshooting 33
- Default Log Locations 33
- Create a Support Bundle for vRealize Automation 34
- Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7 35
- Troubleshooting vRealize Automation Appliances 35
- Troubleshooting Log-In Errors 37

Index 39

Installation and Configuration

The *Installation and Configuration* guide provides information about how to install and configure vRealize Code Stream to automate the release of applications. In this guide, vRealize Automation appliance refers to the underlying appliance with the minimum set of common services required to use the vRealize Code Stream application and vRealize Automation refers to the complete set of capabilities offered by the vRealize Automation product.

Intended Audience

This information is intended for anyone who wants to install vRealize Code Stream, and configure the environment to automate the release applications in development environments. The information is written for experienced developers and operation teams who are familiar with release automation of applications to production environments.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

vRealize Code Stream Installation 1

vRealize Code Stream shares a platform and some common services with vRealize Automation and is delivered in the same virtual appliance.

By entering the appropriate license keys, a System Administrator can unlock either vRealize Automation, vRealize Code Stream or both products on the same appliance.

To install vRealize Code Stream only, you must:

- Deploy and configure a vRealize Automation appliance
- Apply vRealize Code Stream license
- Configure a tenant to assign user roles in vRealize Code Stream

To use the vRealize Code Stream application, a system administrator can deploy a vRealize Automation 7.x appliance and apply a vRealize Code Stream license key.

Note While vRealize Code Stream can be enabled on the same virtual appliance as vRealize Automation in lab or evaluation environments, it is not a recommended nor supported configuration for production systems, particularly when vRealize Automation is configured in High Availability (HA) mode. The current version of vRealize Code Stream does not support HA configuration and, if enabled on a vRealize Automation system in HA mode, can leave the overall system in an unpredictable state.

If you have tried to enable vRealize Code Stream on a vRealize Automation system in HA mode, see the VMware knowledge base article at https://kb.vmware.com/kb/2145084 for the mitigation steps. If you have further questions, please contact VMware Global Support Services.

This chapter includes the following topics:

- "Preparing for Installation," on page 8
- "Using vRealize Code Stream Installation Checklist," on page 11
- "Installation Worksheet," on page 12
- "Installing vRealize Automation with the Installation Wizard," on page 12
- "Installing vRealize Automation through the Standard Interfaces," on page 14
- "Apply a vRealize Code Stream License to an Appliance," on page 19
- "Set Up the Artifactory Server Password," on page 19

Preparing for Installation

System Administrators install vRealize Code Stream into their existing virtualization environments. Before you begin an installation, prepare the deployment environment to meet system requirements.

DNS and Host Name Resolution

vRealize Code Stream requires the system administrator to identify all hosts by using a fully qualified domain name (FQDN).

Important vRealize Code Stream does not allow navigation to hosts that contain the underscore (_) character in the host name.

Hardware and Virtual Machine Requirements

The virtual appliances are pre-configured virtual machines that you add to your vCenter Server or ESXi inventory.

For operating system and high-level environment requirements, including information about supported browsers and operating systems, see the *vRealize Automation Support Matrix*.

An Active Directory is considered small when there are up to 25,000 users in the OU to be synced in the ID Store configuration. An Active Directory is considered large when there are more than 25,000 users in the OU.

The hardware requirements for vRealize Code Stream for Small Active Directories is:

- 4 CPUs
- 18 GB memory
- 60 GB disk storage

Password Considerations

Character restrictions apply to some passwords.

The vRealize Code Stream administrator password is subject to the following restrictions:

- Cannot contain a trailing "=" character. Such passwords are accepted when you assign them, but result in errors when you perform operations such as saving endpoints.
- Cannot contain non-ASCII or extended ASCII characters.
- Cannot contain a comma or have a space between characters.

Port Requirements

vRealize Code Stream uses designated ports for communication and data access.

Although vRealize Code Stream uses only port 443 for communication, there might be other ports open on the system. Because open, unsecure ports can be sources of security vulnerabilities, review all open ports on your system and ensure that only the ports that are required by your business applications are open.

vRealize Automation Appliance

The following ports are used by the vRealize Automation appliance.

Table 1-1. Incoming Ports for the vRealize Automation appliance

Port	Protocol	Comments
22	TCP	Optional. SSH.
80	TCP	Optional. Redirects to 443.
111	TCP, UDP	RPC
443	TCP	Access to the vRealize Automation console and API calls.
5480	TCP	Access to virtual appliance Web management interface
5480	TCP	Used by Management Agent
5488, 5489	TCP	Internal. Used by vRealize Automation appliance for updates.
4369, 25672,5671,5672	TCP	RabbitMQ messaging
8230, 8280, 8281	TCP	Internal vRealize Orchestrator instance
8444	TCP	Console proxy communication for vSphere VMware Remote Console connections

Table 1-2. Outgoing Ports for the vRealize Automation Appliance

Port	Protocol	Comments
25, 587	TCP, UDP	SMTP for sending outbound notification emails
53	TCP, UDP	DNS
67, 68, 546, 547	TCP, UDP	DHCP
80	TCP	Optional. For fetching software updates. Updates can be downloaded separately and applied.
110, 995	TCP, UDP	POP for receiving inbound notification emails
143, 993	TCP, UDP	IMAP for receiving inbound notification emails
123	TCP, UDP	Optional. For connecting directly to NTP instead of using host time.
902	TCP	ESXi network file copy operations and VMware Remote Console (VMRC) connections
5432	TCP, UDP	Optional. For communicating with an Appliance Database.
7444	TCP	Communication with SSO service over HTTPS
8281	TCP	Optional. For communicating with an external vRealize Orchestrator instance .

Other ports might be required by specific vRealize Orchestrator plug-ins that communicate with external systems. See the documentation for the vRealize Orchestrator plug-in.

User Accounts and Credentials Required for Installation

You must verify that you have the roles and credentials to install vRealize Code Stream components.

Virtual Appliance Installation

To deploy the vRealize Automation appliance, you must have the appropriate privileges on the deployment platform (for example, vSphere administrator credentials).

During the deployment process, you specify the password for the virtual appliance administrator account. This account provides access to the vRealize Automation appliance management console from which you configure and administer the virtual appliances.

Security

vRealize Code Stream uses SSL to ensure secure communication among components. Passphrases are used for secure database storage.

Certificates

vRealize Code Stream uses SSL certificates for secure communication among instances of the vRealize Code Stream. You can obtain certificates from an internal or external certificate authority, or generate self-signed certificates during the deployment process for each component.

For important information about troubleshooting, supportability, and trust requirements for certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2106583.

You can update or replace certificates after deployment. For example, a certificate may expire or you may choose to use self-signed certificates during your initial deployment, but then obtain certificates from a trusted authority before going live with your vRealize Code Stream implementation. When you do a minimal deployment, you can generate a self-signed certificate during vRealize Code StreamAppliance configuration.

Certificate Chains

If you use certificate chains, specify the certificates in the following order:

- Client/server certificate signed by the intermediate CA certificate
- One or more intermediate certificates
- A root CA certificate

Include the BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate when you import certificates.

Extracting Certificates and Private Keys

Certificates that you use with the virtual appliances must be in the PEM file format.

The examples in the following table use Gnu `openssl` commands to extract the certificate information you need to configure the virtual appliances.

Table 1-3. Sample Certificate Values and Commands (openssl)

Certificate Authority Provides	Command	Virtual Appliance Entries
RSA Private Key	openssl pkcs12 -in *path _to_.pfx certificate_file* -nocerts -out key.pem	**RSA Private Key**
PEM File	openssl pkcs12 -in *path _to_.pfx certificate_file* -clcerts -nokeys -out cert.pem	**Certificate Chain**
(Optional) Pass Phrase	n/a	**Pass Phrase**

Security Passphrase

vRealize Code Stream uses security passphrases for database security. A passphrase is a series of words used to create a phrase that generates the encryption key that protects data while at rest in the database.

Follow these guidelines when creating a security passphrase for the first time.

- Use the same passphrase across the entire installation to ensure that each component has the same encryption key.

- Use a phrase that is greater than eight characters long.
- Include uppercase, lowercase and numeric characters, and symbols.
- Memorize the passphrase or keep it in a safe place. The passphrase is required to restore database information in the event of a system failure or to add components after initial installation. Without the passphrase, you cannot restore successfully.

Time Synchronization

A system administrator must set up accurate timekeeping as part of the vRealize Code Stream installation.

Installation fails if time synchronization is set up incorrectly.

Timekeeping must be consistent and synchronized across the vRealize Code Stream and remote vRealize Automation servers. By using the same timekeeping method for each component, you can ensure this consistency.

For virtual machines, you can use the following methods:

- Configuration by using Network Time Protocol (directly)
- Configuration by using Network Time Protocol through ESXi with VMware Tools. You must have NTP set up on the ESXi.

For Windows servers, consult Timekeeping best practices for Windows, including NTP.

Using vRealize Code Stream Installation Checklist

The installation checklist provides a high-level overview of the sequence of tasks you must perform to complete the vRealize Code Stream installation.

Installation Checklist

Use the checklist to track your work as you complete the installation tasks in the order they are listed.

Table 1-4. Installation Tasks

Task	Details
Complete the installation worksheet	"Installation Worksheet," on page 12
Deploy the vRealize Automation appliance	"Deploy the vRealize Automation Appliance," on page 12
Set up the vRealize Automation appliance	"Configure the vRealize Automation appliance," on page 17
Add the vRealize Code Stream license key	"Apply a vRealize Code Stream License to an Appliance," on page 19
Set up the Artifactory Server password	"Set Up the Artifactory Server Password," on page 19
Configure Tenant	Configuring Additional Tenants
Add vRealize Code Stream roles	"Assign Roles to Directory Users or Groups," on page 22 Assign the Release Manager, Release Engineer, and Release Dashboard user roles for modeling and publishing a pipeline.
Register the Default Artifactory Server	"Register an Artifactory Server for Artifact Management," on page 27

Installation Worksheet

You can use this worksheet to record important information for reference during the installation process.

The settings that you provide are case sensitive.

Table 1-5. vRealize Automation appliance Information

Variable	Value	Example
Host Name (FQDN)		vrcs-va.mycompany.com
SSO service over HTTPS Outgoing Port (default)	7444 (do not change)	7444
IP		192.168.1.105
Username	administrator@vsphere.local (default)	administrator@vsphere.local
Password		vmware

Installing vRealize Automation with the Installation Wizard

The Installation Wizard for vRealize Automation provides a simple and fast way to install minimal or enterprise deployments.

You must deploy a vRealize Automation appliance before you begin the wizard.

Wizard Navigation

The Installation Wizard appears the first time you log in to your vRealize Automation appliance. If you want to stop the wizard and return later, logout with the **Logout** button that appears on each screen. Use the **Cancel** button to exit the wizard and install through the management console.

Use the **Previous** and **Next** buttons to navigate through wizard screens.

Deploy the vRealize Automation Appliance

To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.

Some restrictions apply to the root password you create for the vRealize Automation administrator.

For more information, see "Password Considerations," on page 8.

Prerequisites

- Download the vRealize Automation appliance from the VMware Web site.
- Log in to the vSphere client as a user with system administrator privileges.

Procedure

1. Select **File > Deploy OVF Template** from the vSphere client.
2. Browse to the vRealize Automation appliance file you downloaded and click **Open**.
3. Click **Next**.
4. Click **Next** on the OVF Template Details page.
5. Accept the license agreement and click **Next**.

6 Enter a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.

7 Follow the prompts until the Disk Format page appears.

8 Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.

9 Select the disk format. For example, Thin Provisioning.

10 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

11 Configure the values on the Properties page.

a Enter the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.

b Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

This value is used to set the initial status of the SSH service in the appliance. If you are installing with the Installation Wizard, enable this before you begin the wizard. You can change this setting from the appliance management console after installation.

c Enter the fully qualified domain name of the virtual machine in the **Hostname** text box, even if you are using DHCP.

d Configure the networking properties.

12 Click **Next**.

13 Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.

- If **Power on after deployment** is available on the Ready to Complete page.

  a Select **Power on after deployment** and click **Finish**.

  b Click **Close** after the file finishes deploying into vCenter.

  c Wait for the machine to start.

  This could take up to 5 minutes.

- If **Power on after deployment** is not available on the Ready to Complete page.

  a Click **Close** after the file finishes deploying into vCenter.

  b Power on the VM and wait for some time for the VM to start up.

  c Verify that you can ping the DNS of the virtual machine. If you cannot ping the DNS, restart the virtual machine.

  d Wait for the machine to start. This could take up to 5 minutes.

14 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Automation appliance.

Run the Installation Wizard for a Minimal Deployment

Set up a single vRealize Automation appliance to install vRealize Code Stream.

The wizard is disabled when you click **Cancel**, or when you log out of the wizard and begin an installation through the management console.

Procedure

1 Open a Web browser.

2 Navigate to the vRealize Automation management console by using its fully qualified domain name, https://*vrcs-vahostname.domain.name*:5480/.

3 Log in with the user name **`root`** and the password you specified when the appliance was deployed.

4 When the Installation Wizard appears, click **Next**.

5 Accept the End User License Agreement and click **Next**.

6 Select **Minimal Deployment** and unselect **Install Infrastructure as a Service** on the Deployment Type screen and click **Next**.

7 If needed, you can change the timekeeping method for your vRealize Automation appliance. Click **Change Time Settings,** if you make changes.

8 Select **Resolve Automatically** to select the host.

9 Enter the administration password, confirm the password and click **Next**.

10 Submit the vRealize Appliance Certificate information such as Oraganization, Oraganizational Unit and Country code.

11 Click on Save Generated Certificate and click **Next**.

12 Click **Install**.

13 Enter a valid vRealize Code Stream license key and click **Submit Key**.

The default Artifactory server is enabled when the valid license key is accepted.

The vRealize Code Stream license includes the Artifactory Pro version.

14 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).

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.

15 (Optional) Select **Join the VMware Customer Experience Improvement Program to participate in the program** and click **Next**.

16 Click **Next**.

17 Click **Finish**.

18 Confirm that you can log in to the vRealize Automation console.

a Open a Web browser.

b Navigate to *https://vrcs-hostname.domain.name/vcac*.

Installing vRealize Automation through the Standard Interfaces

As an alternative to the Installation Wizard, you can install vRealize Automation through the vRealize Automation appliance management console.

Installation through the standard interface is intended primarily for minimal deployment.

Minimal Deployment Checklist

A system administrator can deploy complete product in a minimal configuration. Minimal deployments are typically used in a development environment or as a proof of concept and require fewer steps to install.

The Minimal Deployment Checklist provides a high-level overview of the sequence of tasks you must perform to complete a minimal installation.

Print out a copy of the checklist and use it to track your work as you complete the installation. Complete the tasks in the order in which they are given.

Table 1-6. Minimal Deployment Checklist

	Task	Details
❑	Plan and prepare the installation environment and verify that all installation prerequisites are met.	"Password Considerations," on page 8
❑	Set up your vRealize Automation appliance	"Deploy and Configure the vRealize Automation Appliance," on page 15

Deploy and Configure the vRealize Automation Appliance

The vRealize Automation appliance is a preconfigured virtual appliance that deploys the vRealize Automation appliance server and Web console (the user portal). It is delivered as an open virtualization format (OVF) template. The system administrator downloads the appliance and deploys it into the vCenter Server or ESX/ESXi inventory.

Deploy the vRealize Automation Appliance

To deploy the vRealize Automation appliance, a system administrator must log in to the vSphere client and select deployment settings.

Some restrictions apply to the root password you create for the vRealize Automation administrator.

For more information, see "Password Considerations," on page 8.

Prerequisites

- Download the vRealize Automation appliance from the VMware Web site.
- Log in to the vSphere client as a user with system administrator privileges.

Procedure

1. Select **File > Deploy OVF Template** from the vSphere client.
2. Browse to the vRealize Automation appliance file you downloaded and click **Open**.
3. Click **Next**.
4. Click **Next** on the OVF Template Details page.
5. Accept the license agreement and click **Next**.
6. Enter a unique virtual appliance name according to the IT naming convention of your organization in the **Name** text box, select the datacenter and location to which you want to deploy the virtual appliance, and click **Next**.
7. Follow the prompts until the Disk Format page appears.
8. Verify on the Disk Format page that enough space exists to deploy the virtual appliance and click **Next**.

9 Follow the prompts to the Properties page.

The options that appear depend on your vSphere configuration.

10 Configure the values on the Properties page.

a Enter the root password to use when you log in to the virtual appliance console in the **Enter password** and **Confirm password** text boxes.

b Select or uncheck the **SSH service** checkbox to choose whether SSH service is enabled for the appliance.

This value is used to set the initial status of the SSH service in the appliance. If you are installing with the Installation Wizard, enable this before you begin the wizard. You can change this setting from the appliance management console after installation.

c Enter the fully qualified domain name of the virtual machine in the **Hostname** text box, even if you are using DHCP.

d Configure the networking properties.

11 Click **Next**.

12 Depending on your vCenter and DNS configurations, it could take some time for the DNS to resolve. To expedite this process, perform the following steps.

- If **Power on after deployment** is available on the Ready to Complete page.
  a Select **Power on after deployment** and click **Finish**.
  b Click **Close** after the file finishes deploying into vCenter.
  c Wait for the machine to start.

  This could take up to 5 minutes.
- If **Power on after deployment** is not available on the Ready to Complete page.
  a Click **Close** after the file finishes deploying into vCenter.
  b Power on the VM and wait for some time for the VM to start up.
  c Verify that you can ping the DNS of the virtual machine. If you cannot ping the DNS, restart the virtual machine.
  d Wait for the machine to start. This could take up to 5 minutes.

13 Open a command prompt and ping the FQDN to verify that the fully qualified domain name can be resolved against the IP address of vRealize Automation appliance.

Enable Time Synchronization on the vRealize Automation Appliance

To ensure a successful installation, enable time synchronization on the Clocks on the vRealize Automation Appliance.

If you see certificate warnings during this process, continue past them to finish the installation.

Prerequisites

"Deploy the vRealize Automation Appliance," on page 15.

Procedure

1 Navigate to the vRealize Automation management console by using its fully qualified domain name, https://*vrcs-vahostname.domain.name*:5480/.

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

3 Select **Admin > Time Settings**.

4 Select an option from the **Time Sync Mode** menu.

Option	Action
Use Time Server	Select **Use Time Server** from the **Time Sync Mode** menu to use Network Time Protocol . For each time server that you are using, enter the IP address or the host name in the **Time Server** text box.
Use Host Time	Select **Use Host Time** from the **Time Sync Mode** menu to use VMware Tools time synchronization. You must configure the connections to Network Time Protocol servers before you can use VMware Tools time synchronization.

5 Click **Save Settings**.

6 Click **Refresh**.

7 Verify that the value in **Current Time** is correct.

You can change the time zone as required from the Time Zone Setting page on the **System** tab.

8 (Optional) Click **Time Zone** from the **System** tab and select a system time zone from the menu choices.

The default is Etc/UTC.

9 Click **Save Settings**.

Configure the vRealize Automation appliance

To prepare the vRealize Automation appliance for use, a system administrator configures the host settings, generates an SSL certificate, and provides SSO connection information.

Procedure

1 Navigate to the vRealize Automation management console by using its fully qualified domain name, https://*vrcs-vahostname.domain.name*:5480/.

2 Continue past the certificate warning.

3 Log in with user name root and the password you specified when you deployed vRealize Automation appliance.

4 Select **vRA Settings > Host Settings**

Option	Action
Resolve Automatically	Select **Resolve Automatically** to specify the name of the current host for the vRealize Automation vRealize Automation appliance.
Update Host	For new hosts, select **Update Host**. Enter the fully qualified domain name of the vRealize Automation appliance, *vrcs-hostname.domain.name*, in the **Update Host** text box.

Note Configure SSO settings as described later in this procedure whenever you use **Update Host** to change a host name.

5 Select the certificate type from the **Certificate Action** menu.

If you are using a PEM-encoded certificate, for example for a distributed environment, select **Import**.

Certificates that you import must be trusted and must also be applicable to all instances of vRealize Automation appliance through the use of Subject Alternative Name (SAN) certificates.

Note If you use certificate chains, specify the certificates in the following order:

a Client/server certificate signed by the intermediate CA certificate

b One or more intermediate certificates

c A root CA certificate

Option	Action
Keep Existing	Leave the current SSL configuration. Select this option to cancel your changes.
Generate Certificate	a The value displayed in the **Common Name** text box is the Host Name as it appears on the upper part of the page. If any additional instances of the vRealize Automation appliance available, their FQDNs are included in the SAN attribute of the certificate. b Enter your organization name, such as your company name, in the **Organization** text box. c Enter your organizational unit, such as your department name or location, in the **Organizational Unit** text box. d Enter a two-letter ISO 3166 country code, such as **US**, in the **Country** text box.
Import	a Copy the certificate values from BEGIN PRIVATE KEY to END PRIVATE KEY, including the header and footer, and paste them in the **RSA Private Key** text box. b Copy the certificate values from BEGIN CERTIFICATE to END CERTIFICATE, including the header and footer, and paste them in the **Certificate Chain** text box. For multiple certificate values, include a BEGIN CERTIFICATE header and END CERTIFICATE footer for each certificate. **Note** In the case of chained certificates, additional attributes may be available. c (Optional) If your certificate uses a pass phrase to encrypt the certificate key, copy the pass phrase and paste it in the **Passphrase** text box.

6 Click **Save Generated Certificate** if you have selected the follow the **Generated Certificate** option.

7 Follow the on-screen prompts if you have selected the **Keep Existing** option.

8 Enter a new license key for vRealize Code Stream.

9 Click **Submit Key** and click **Next**.

10 Click the **Telemetry** tab to choose whether to join the VMware Customer Experience Improvement Program (CEIP).

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.

11 (Optional) Select **Join the VMware Customer Experience Improvement Program to participate in the program** and click **Next**.

12 Click **Next**.

13 Click **Finish**.

Apply a vRealize Code Stream License to an Appliance

When you apply the vRealize Code Stream standalone license to a vRealize Automation appliance, you enable the vRealize Code Stream functions.

You can use the vRealize Code Stream standalone license to enable the Artifact Management, Release Management, Release Dashboard, Approval Services, and Advanced Service Designer features.

Prerequisites

Verify that the vRealize Automation appliance is set up. See "Configure the vRealize Automation appliance," on page 17.

Procedure

1 Open the vRealize Automation Appliance management console with the fully qualified domain name, https:// *vrcs-va-hostname.domain.name*:5480/.

2 Log in as the root user.

3 Select **vRA Settings > Licensing**.

4 Enter a valid vRealize Code Stream license key and click **Submit Key**.

The default Artifactory server is enabled when the valid license key is accepted.

The vRealize Code Stream license includes the Artifactory Pro version.

5 Confirm that you can log in to the vRealize Automation console.

a Open a Web browser.

b Navigate to https://*vrcs-hostname.domain.name*/vcac.

What to do next

Configure a repository in the Artifactory server. See the JFrog Web site https://www.jfrog.com/confluence/display/RTF/Configuring+Repositories.

Set Up the Artifactory Server Password

The default Artifactory server is enabled when you apply the vRealize Code Stream license to the appliance. For security purposes, change the default login credentials.

The vRealize Code Stream license includes the Artifactory Pro version.

Procedure

1 Open a Web browser.

2 Type the **`https://vrcs-hostname/artifactory/`** URL.

3 Log in using the default username **`vmadmin`** and password **`vmware`**.

4 Click the **Admin** tab and click **Users** in the left pane.

5 Select the **vmadmin** user name.

6 Change the default login credentials.

Note You will require the password when you configure the Artifactory end points.

7 Click **Save.**

8 Log out.

Configuring Components 2

You must configure components such as vRealize Automation tenants, assign roles to the identity store, and configure the Artifactory server before you can use vRealize Code Stream.

You create the default tenant when you install vRealize Automation, but you can create additional tenants to represent business units in an enterprise or companies that subscribe to cloud services from a service provider. For more information on configuring tenants, see *Installing vRealize Automation 7.0*.

This chapter includes the following topics:

- "Managing Users," on page 21
- "Configure a Tenant to a User in the Artifactory Server," on page 24
- "Configure an External Disk Partition for the Artifactory Server," on page 25
- "Publish a Service Blueprint as a Catalog Item," on page 25

Managing Users

Tenant administrators create and manage custom groups and grant and manage user access rights to the vRealize Automation console.

Add Identity Store

vRealize Automation uses identity stores to authenticate users. Each tenant is associated with at least one identity store when it is created, but you can add new ones if necessary.

When you delete an identity store, this removes the roles assigned to users from this store, the roles assigned to users from custom groups, and the information about which services are available to this user. Entries for entitlements and business groups are not affected.

Prerequisites

Log in to the vRealize Automation console as a **tenant administrator**.

Procedure

1 Select **Administration > Directories Management > Directories**.

2 Click the **Add** icon ( ).

3 Enter a name in the **Name** text box.

4 Select the type of the identity store from the **Type** drop-down menu.

5 Enter the following Identify Store configuration options.

Option	Action
URL	Enter the URL for the identity store. For example, `ldap://10.141.64.166:875`.
Domain	Enter the domain for the identity store.
(Optional) Domain Alias	Enter the domain alias.
Login User DN	Enter the login user Distinguished Name. For example, `cn=demoadmin,ou=demo,dc=dev,dc=mycompany,dc=com`.
Password	Enter the password for the identity store login user.
Group Search Base DN	Enter the group search base Distinguished Name. For example, `ou=demo,dc=dev,dc=mycompany,dc=com`.
User Search Base DN	Enter the user search base Distinguished Name.

6 Click **Test Connection**.

7 Click **Add**.

What to do next

"Assign Roles to Directory Users or Groups," on page 22.

Assign Roles to Directory Users or Groups

Tenant administrators grant users access rights by assigning roles to users or groups.

Prerequisites

Log in to the vRealize Automation console as a **tenant administrator**.

Procedure

1 Select **Administration > Users & Groups > Directory Users & Groups**.

2 Enter a user or group name in the **Search** box and press Enter.

Do not use an at sign (@), backslash (\), or slash (/) in a name. You can optimize your search by typing the entire user or group name in the form user@domain.

3 Click the name of the user or group to which you want to assign roles.

4 Select one or more roles from the Add Roles to this User list.

The Authorities Granted by Selected Roles list indicates the specific authorities you are granting.

5 (Optional) Click **Next** to view more information about the user or group.

6 Click **Update**.

Users who are currently logged in to the vRealize Automation console must log out and log back in to the vRealize Automation console before they can navigate to the pages to which they have been granted access.

What to do next

Optionally, you can create your own custom groups from users and groups in your Active Directory connections. See "Create a Custom Group," on page 23.

Create a Custom Group

Tenant administrators can create custom groups by combining other custom groups, identity store groups, and individual identity store users.

You can assign roles to your custom group, but it is not necessary in all cases. For example, you can create a custom group called Machine Specification Approvers, to use for all machine pre-approvals. You can also create custom groups to map to your business groups so that you can manage all groups in one place. In those cases, you do not need to assign roles.

Prerequisites

Log in to the vRealize Automation console as a **tenant administrator**.

Procedure

1 Select **Administration > Users & Groups > Custom Groups**.

2 Click the **Add** icon ().

3 Enter a group name in the **New Group Name** text box.

Custom group names cannot contain the combination of a semicolon (;) followed by an equal sign (=).

4 (Optional) Enter a description in the **New Group Description** text box.

5 Select one or more roles from the Add Roles to this Group list.

The Authorities Granted by Selected Roles list indicates the specific authorities you are granting.

6 Click **Next**.

7 Add users and groups to create your custom group.

a Enter a user or group name in the **Search** box and press Enter.

Do not use an at sign (@), backslash (\), or slash (/) in a name. You can optimize your search by typing the entire user or group name in the form user@domain.

b Select the user or group to add to your custom group.

8 Click **Add**.

Users who are currently logged in to the vRealize Automation console must log out and log back in to the vRealize Automation console before they can navigate to the pages to which they have been granted access.

Manage User and Group Entitlements

You can use user and group directory name search parameters to control user and group entitlements.

If users or groups from other domains do not possess the expected system privileges, and do not appear on the **Administration > Users** page or the **Administration > Groups** page, check the user and group search base distinguished name parameters on the Identity Store Configuration page. Ensure that the distinguished name search parameters are not so restrictive that the users and groups are excluded the desired domains.

Prerequisites

Log in to vRealize Automation as a tenant administrator.

Procedure

1 Select **Administration > Identity Stores** .

2 Select the appropriate identity store and then click the **Edit** button.

3 Edit the group base distinguished name search parameters in the **Group search base DN** field.

If users or groups do not possess adequate privileges, edit the search parameters to be less restrictive.

4 Edit the user base distinguished name search parameters in the **User search base DN** field.

If users or groups do not possess adequate privileges, edit the search parameters to be less restrictive.

5 Click **Test Connection**.

6 Click **Update**.

Configure a Tenant to a User in the Artifactory Server

For organizations that have Artifactory with multiple repositories, a tenant administrator can map a vRealize Automation tenant to the corresponding user in the Artifactory server from the vRealize Code Stream user interface. The mapping lets the organization control the access to the Artifactory repository among its users.

The Artifactory administrator can set up permissions which include the group, user, and the Artifactory repository.

Important The Artifactory users must belong to the vRealize group in Artifactory.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator**.

  If you are mapping users for a different tenant such as Dev-Artifactory tenant, log out and log in as that tenant.

- Verify that the Artifactory repositories, users, and groups are configured. See the *Artifactory User Guide* on the jFrog Web site.

Procedure

1 Select **Administration > Artifact Management**.

2 Enter a name for the Artifactory server.

You can add notes that apply to the server in the Description section.

3 Enter the URL of the Artifactory server.

The server URL format is https://vra-*hostname*/artifactory.

4 Enter the Artifactory user name to map that user to the tenant.

You can add notes that apply to the user and tenant in the Description section.

5 Enter a name for the Artifactory server.

You can add notes that apply to the server in the Description section.

6 Enter the Artifactory password set for the user.

7 Select the artifact and click **Test Connection** to verify that the appliance can connect to the Artifactory server.

8 Click **Update** to save your changes.

What to do next

You can create a remote repository and map it to the remote repository in the embedded vRealize Code Stream Artifactory server. To create a remote repository on the jFrog Web site, see the *Configuring Artifactory* guide.

Configure an External Disk Partition for the Artifactory Server

If you plan to store large binaries you can configure external disk partition to the default Artifactory server and synchronize the existing artifacts.

The local storage in the appliance is 25 GB.

Prerequisites

- Verify that you have a vRealize Automation host.
- Verify that the NFS share path is available with adequate storage.

Procedure

1 Open a terminal and SSH in the vRealize Automation host using root@*VRA-host-name*.

2 Type the vRealize Automation appliance password.

3 Stop the artifactory server.

```
/opt/jfrog/artifactory/bin/artifactroy.sh stop
```

4 Mount the NFS share to the vRealize Automation host.

```
mount NFS-server-host-name:/host/NFS-share-host-path /mount/VRA-path
```

5 Navigate to the `/opt/jfrog/artifactory/misc/db/postgresql.properties` file.

6 Uncomment the binary.provider.type entry in the file.

```
binary.provider.type=filesystem
```

7 Add the new NFS share path in the file.

```
binary.provider.filesystem.dir=NFS-share-path
```

8 Restart the artifactory server.

```
/opt/jfrog/artifactory/bin/artifactroy.sh start
```

What to do next

Synchronize the existing artifacts to the new external disk partition. See Changing the Default Storage topic on the JFrog Web site.

Publish a Service Blueprint as a Catalog Item

After you create a service blueprint, it is in a draft state and you can publish it as a catalog item.

Prerequisites

Log in to the vRealize Automation console as an **XaaS architect**.

Procedure

1 Select **Design > XaaS > XaaS Blueprints**.

2 Select the row of the service blueprint to publish, and click **Publish**.

The status of the service blueprint changes to Published.

3 (Optional) Select **Administration > Catalog Management > Catalog Items** to view the published catalog item.

Registering Components 3

You must register various components such as plug-ins, endpoints, and the Artifactory server before you can model and run release pipelines in vRealize Code Stream.

This chapter includes the following topics:

- "Register an Artifactory Server for Artifact Management," on page 27
- "Registering Plug-In Instances and Endpoints for a Release Pipeline," on page 28

Register an Artifactory Server for Artifact Management

To use artifact management in a release pipeline, you must connect to an Artifactory server.

With artifact management, you can specify an artifact by name and search type from the server, but not by location or unique identifier. Artifact management monitors the physical location and identity of artifacts and supplies the required artifact during the pipeline execution.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator**.
- Verify that the Artifactory server is not using the default login credentials. See "Set Up the Artifactory Server Password," on page 19.
- Verify that the tenant role is assigned for the **Release Automation** and **Release Dashboard** tabs to appear in the appliance user interface. See Configuring Additional Tenants.
- Verify that the Artifactory server is configured. See the *Artifactory User Guide* on the jFrog Web site.

Procedure

1 Select **Administration > Artifact Management**.

2 Enter a name for the Artifactory server.

You can add notes that apply to the server in the Description section.

3 Enter the URL of the Artifactory server.

The server URL format is https://*vrcs-hostname*/artifactory.

4 Enter the Artifactory user name to map that user to the tenant.

You can add notes that apply to the user and tenant in the Description section.

5 Enter the Artifactory password set for the user.

> **Note** The Admin password expires at first login. After you login for the first time with default credentials, you must change the password before you proceed to the next task. You must change the password in the Artifactory server before you configure the endpoint in vRealize Code Stream.

6 Select the artifact and click **Test Connection** to verify that the appliance can connect to the Artifactory server.

7 Click **Update** to save your changes.

The release pipeline can access the Artifactory server.

Registering Plug-In Instances and Endpoints for a Release Pipeline

You must define and configure the plug-in instance or endpoint before you create a task in a release pipeline.

A plug-in instance allows parameters to be defined in the custom task. You can access the custom workflow in the vRealize Orchestrator client when you execute the pipeline.

An endpoint allows the parameters defined in the provision or test tasks in the release pipeline to access the vRealize Automation server or Jenkins server when you run the pipeline.

Register a Jenkins Server Endpoint

You can run tests or other jobs by using the Jenkins plug-in that allows you to use custom automation and scripts.

You can use any Jenkins job in the Jenkins server in the release pipeline with this endpoint enabled. You can use this endpoint to invoke a Jenkins build job during the modeling of a release pipeline and execute the job as part of the release pipeline.

Register a Jenkins Server Endpoint (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrcs_register_jenkins)

Prerequisites

- Verify that the Jenkins server is available and configured with or without SSL.
- Verify that the Jenkins server version is 1.561 or later.
- Verify that the Jenkins jobs are created in the Jenkins server with the input string parameter, vRCSTestExecutionId.
- Log in to the vRealize Automation console as a **system administrator** or **release manager**.

Procedure

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

2 Click **Add**.

3 Select **Jenkins (Code Stream)** from the **Plug-In** drop-down menu and click **Next**.

4 Enter a Jenkins server endpoint name and an applicable description.

For example, in the description section you can add the release pipeline name that uses this Jenkins server endpoint.

5 Click **Next**.

6 Enter the Jenkins server configuration details.

Option	Description
Jenkins Instance Name	Enter the Jenkins instance name. For example, qe-jenkins.test.com.
User Credentials	User name and password for the Jenkins server.
URL	Enter the host URL as *protocol://host:port*. Sample host URL, 192.10.121.13:8080.
Polling Interval	Time that the task must wait to check the progress.
Request Retry Count	Number of times to retry the scheduled build request for the Jenkins server.
Retry Wait Time	Seconds to wait before retrying the build request for the Jenkins server.
Offline Creation	Require a validation and certificate acceptance when the endpoint is created. You can accept the default setting or select **Yes** from the drop-down menu to enable this configuration.

7 Click **Add**.

8 Click the **Code Stream** tab in vRealize Automation to continue with the task configuration.

What to do next

Create a test task to use this endpoint in the release pipeline. See the *Using vRealize Code Stream* guide.

Register a vRealize Automation Server Endpoint

When you register a vRealize Automation, vRealize Code Stream invokes vRealize Automation 6.2 or 7.0 instance to provision infrastructure in a specific environment

vRealize Code Stream can also invoke multiple vRealize Automation instances.

You must register a vRealize Automation server endpoint to provision a machine blueprint on vRealize Automation.

Register a vRealize Automation Server Endpoint (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrcs_register_vra)

Prerequisites

- Log in to the vRealize Automation console as a **system administrator** or **release manager**.

Procedure

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

2 Click **Add**.

3 Select **vRA Provisioning (Code Stream)** from the Plug-in drop-down menu and click **Next**.

4 Enter a vRealize Automation endpoint name and an applicable description.

5 Click **Next**.

6 Enter the vRealize Automation server configuration details.

Option	Description
vRA Instance Name	Enter the vRealize Automation instance name.
Polling Interval	Time that the task must wait to check the progress.
Maximum Wait for IP assignment	Time that the task must wait for the IP addresses to be assigned to a machine before it can report the failure.

7 Click **Next**.

8 Define the user credentials for the vRealize Automation instance authentication.

- Select **Shared session** from the drop-down menu to use provisioned blueprints from a remote vRealize Automation instance.

  You must provide the secure vRealize Automation host and port URL, the tenant name, and the user credentials of the user sharing the session for instance authentication.

  Note Select share session to use provisioned blueprints from a remote vRealize Automation instance using a different identity appliance than vRealize Code Stream.

9 Click **Add**.

10 Select the **Code Stream** tab invRealize Automation to continue with the task configuration.

What to do next

Create a provision task to use this endpoint in the release pipeline. See the *Using vRealize Code Stream* guide.

Register a vRealize Orchestrator Workflow for a Custom Task

With the vRealize Orchestrator workflow plug-in for the custom task, you can use any of the custom workflows defined in vRealize Orchestrator service on the vRealize Code Stream appliance. You can select the custom workflow, configure it, and use it in the release pipeline model.

Prerequisites

- Verify that the workflow for a custom workflow is created in vRealize Orchestrator.

Procedure

1 Log in to the vRealize Orchestrator client to create a workflow.

2 Select **Library** > **Tagging** > **Tag workflow**.

The Tag workflow is required for custom user workflows.

By default, the Manual Task workflow is provided.

3 Right-click the **Tag workflow** and select **Start Workflow**.

4 Click the **Tagged Workflow** text box to select the custom workflow.

For example, the tagged workflow can be Deploy Spring Travel.

5 Enter the tag as **vRCS_CUSTOM**.

6 Enter the value as **vRCS_CUSTOM**.

7 Click **Yes** for the Global tag and click **Submit**.

8 Click the **Code Stream** tab in vRealize Automation to continue with the task configuration.

Register a vRealize Orchestrator Workflow for a Gating Rule

With the vRealize Orchestrator workflow plug-in for gating rules, you can use any workflow as a gating rule workflow from release automation. You can select the custom workflow, configure it with the vRCS_GATING_RULE tag, and use it to model the release pipeline and execute the release pipeline.

Prerequisites

- Verify that the workflow for vRCS_GATING_RULE Workflow is created.

Procedure

1. Log in to the vRealize Orchestrator client to create a workflow.
2. Select **Library** > **Tagging** > **Tag workflow**.
3. Right-click the **Tag workflow** and select **Start Workflow**.
4. Click the **Tagged Workflow** text box to select the **vRCS_GATING_RULE** workflow.
5. Enter the tag as **vRCS_GATING_RULE**.
6. Enter the value as **vRCS_GATING_RULE**.
7. Click **Yes** for the Global tag and click **Submit**.
8. Click the **Code Stream** tab in vRealize Automation to continue with the task configuration.

Register a Team Foundation Server Endpoint

You can connect to the Team Foundation Server plug-in to manage version control, track defects and work items, and manage your build projects.

Prerequisites

Verify that you have installed and configured Visual Studio Team Foundation Server 2013 or 2015.

Procedure

1. Select **Administration > Orchestration Configuration > Endpoints**.
2. Click **Add**.
3. Select **Team Foundation Server (Code Stream)** from the Plug-in drop-down menu and click **Next**.
4. Enter an Team Foundation Server endpoint name and an applicable description.
5. Click **Next**.
6. Enter the Team Foundation Server configuration details.

Option	Description
Team Foundation Server Instance Name	Enter the Team Foundation Server instance name. For example, qe-tfs-test
User Credentials	User name and password for the Team Foundation Server.
Domain Name	Domain name for the Team Foundation Server. If the Team Foundation Server is not in a domain, you can use the Windows server host name.
URL	Enter the host URL as *protocol://host:port*/tfs. For example, http://192.10.121.12:8080/tfs or https://192.10.121.12:8080/tfs
Polling Interval	Time that the task must wait to check the progress.

Option	Description
Offline Creation	Require a validation and certificate acceptance when the endpoint is created. You can accept the default setting or select **Yes** from the drop-down menu to enable this configuration.
TFS Server Version	Select the TFS Server version as 2013 or 2015. Your selection of the TFS Server Version is validated and a you will notice an error message if you select an incorrect version.

7 Click **Add**.

8 Select the **Code Stream** tab in vRealize Automation to continue with the task configuration.

What to do next

Create a provision task to use this endpoint in the release pipeline. See the *Using vRealize Code Stream* guide.

4 Troubleshooting

vRealize Code Stream troubleshooting provides procedures for resolving issues you might encounter when installing or configuring vRealize Automation.

This chapter includes the following topics:

- "Default Log Locations," on page 33
- "Create a Support Bundle for vRealize Automation," on page 34
- "Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7," on page 35
- "Troubleshooting vRealize Automation Appliances," on page 35
- "Troubleshooting Log-In Errors," on page 37

Default Log Locations

Consult system and product log files for information on a failed installation.

The file paths shown are the default paths. If you installed IaaS in another directory, navigate to your custom installation directory instead.

Note The VMware vRealize ™ Automation (vRA) content pack for vRealize Log Insight provides a consolidated summary of log events in all of the vRealize Automation components. For more information, see the vRA 6.1+ Log Insight Content Pack description on VMware Solution Exchange at https://solutionexchange.vmware.com/store/products/vra-6-1-log-insight-content-pack#.VU0r3_PD-Ht.

Installation Logs

Installation logs are in the following locations.

Log	Default Location
Installation Logs	`C:\Program Files (x86)\vCAC\InstallLogs` `C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log`
WAPI Installation Logs	`C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>`

IaaS Logs

IaaS logs are in the following locations.

Log	Default Location
Website Logs	`C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs`
Repository Log	`C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs`
Manager Service Logs	`C:\Program Files (x86)\VMware\vCAC\Server\Logs`
DEM Orchestrator Logs	`C:\Users\svc-admin\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\atdhl-ms1-70.sqa.local DEO \Logs`
Agent Logs	`C:\Users\svc-admin\AppData\Local\Temp\VMware\vCAC\Agents\<agent_name>\logs`

vRealize Automation Framework Logs

Log entries for vRealize Automation Frameworks are located in the following location.

Log	Default location
Framework Logs	`/var/log/vmware`

Software Component Provisioning Logs

Software component provisioning logs are located in the following location.

Log	Default Location
Software Agent Bootstrap Log	`/opt/vmware-appdirector (for Linux) or \opt\vmware-appdirector (for Windows)`
Software Lifecycle Script Logs	`/tmp/taskId` (for Linux) `\Users\darwin\AppData\Local\Temp\taskId` (for Windows)

Collection of Logs for Distributed Deployments

You can create a zip file that bundles all logs for components of a distributed deployment. .

Create a Support Bundle for vRealize Automation

A root user can create a support bundle in the vRealize Automation appliance management console. These bundles can help VMware support staff to identify causes of issues you might encounter.

Use the following procedure to create a support bundle for vRealize Automation appliance.

Procedure

1 Navigate to the vRealize Automation appliance management console by using its fully qualified domain name, https://*vrcs-va-hostname.domain.name*:5480/.

2 Log in and go to **Admin > Logs**.

3 Click **Create support bundle**.

4 Click **Download** and save the file on your system.

You can use the support bundle to troubleshoot issues on your own or to send to your VMware support representative.

Blank Pages May Appear When Using Internet Explorer 9 or 10 on Windows 7

When you use Internet Explorer 9 or 10 on Windows 7 and compatibility mode is enabled, some pages appear to have no content.

Problem

When using Internet Explorer 9 or 10 on Windows 7, the following pages have no content:

- Default Tenant Folder on the Orchestrator page
- Server Configuration on the Orchestrator page

Cause

The problem could be related to compatibility mode being enabled. You can disable compatibility mode for Internet Explorer with the following steps.

Solution

Prerequisites

Ensure that the menu bar is displayed. If you are using Internet Explorer 9 or 10, press Alt to display the Menu bar (or right-click the Address bar and then select **Menu bar**).

Procedure

1 Select **Tools > Compatibility View settings**.

2 Deselect **Display intranet sites in Compatibility View**.

3 Click **Close**.

Troubleshooting vRealize Automation Appliances

The troubleshooting topics for vRealize Automation appliances provide solutions to potential installation-related problems that you might encounter when using your vRealize Automation appliances.

Encryption.key File has Incorrect Permissions

A system error can result when incorrect permissions are assigned to the Encryption.key file for a virtual appliance.

Problem

You log in to vRealize Automation appliance and the Tenants page is displayed. After the page has begun loading, you see the message `System Error`.

Cause

The Encryption.key file has incorrect permissions or the group or owner user level is incorrectly assigned.

Solution

Prerequisites

Log in to the virtual appliance that displays the error.

Note If your virtual appliances are running under a load balancer, you must check each virtual appliance.

Procedure

1 View the log file `/var/log/vcac/catalina.out` and search for the message `Cannot write to /etc/vcac/Encryption.key`.

2 Go to the `/etc/vcac/` directory and check the permissions and ownership for the Encryption.key file. You should see a line similar to the following one:

```
-rw------- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Read and write permission is required and the owner and group for the file must be `vcac`.

3 If the output you see is different, change the permissions or ownership of the file as needed.

What to do next

Log in to the Tenant page to verify that you can log in without error.

Identity Manager Fails to Start After Horizon-Workspace Restart

In a vRealize Automation high availability environment, the Identity Manager can fail to start after the horizon-workspace service is restarted.

Problem

The horizon-workspace service cannot start due an error similar to the following:

Error creating bean with name 'liquibase' defined in class path resource [spring/datastore-wireup.xml]: Invocation of init method failed; nested exception is liquibase.exception.LockException: Could not acquire change log lock. Currently locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15

Cause

The Identity Manager may fail to start in a high availability environment due to issues with the liquibase data management utility used by vRealize Automation.

Solution

1 Log in to the vRealize Automation appliance as root using ssh.

2 Run the `service horizon-workspace` command to stop the horizon-workspace service.

3 Run the `su postgres` command to become a postgres user.

4 Run the command `psql vcac`.

5 Run the following SQL query: `"update "databasechangeloglock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`

6 Run the SQL query `select *` from databasechangeloglock.

The output should show a value of "f" for locked.

7 Start the horizon-workspace service using the command `service horizon-workspace start`.

Troubleshooting Log-In Errors

The troubleshooting topics for log-in errors for vRealize Automation provide solutions to potential installation-related problems that you might encounter when using vRealize Automation.

Cannot Log in to a Tenant or Tenant Identity Stores Disappear

Ninety days after deployment, you cannot log into a tenant or the identity store for a tenant disappears.

Problem

- When you log in to a tenant, you see a blank page displayed with a Submit button in the upper left-hand corner.
- You receive a System Exception error when accessing the tenant ID store configuration page.
- The ID store configuration disappears.
- You cannot log in to a tenant by using an LDAP account.
- The `catalina.out` log located in `/var/log/vmware/vcac/` shows an error similar to the following:

```
12:40:49,190 [tomcat-http--34] [authentication] INFO
com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl
$RequestResponseProcessor.handleFaultCondition:922 - Failed trying to retrieve token:
ns0:RequestFailed: Error occurred looking for solution user :: Insufficient access YYYY-03-18
12:40:49,201 [tomcat-http--34] [authentication] ERROR
com.vmware.vcac.platform.service.rest.resolver.ApplicationExceptionHandler.handleUnexpectedEx
ception:820 - Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for
solution user :: Insufficient access com.vmware.vim.sso.client.exception.InternalError:
Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for solution
user :: Insufficient access
```

Cause

The SSO internal tenant administrator password expires after 90 days by default. This issue is internal to vRealize Automation and does not affect external, Active Directory identity stores.

It is a known issue that the vRealize Automation user interface does not provide notification that the tenant administrator password is expiring. The workaround for this issue is to disable password expiration for the tenant administrator account.

For step-by-step instructions to resolve this issue, see the VMware knowledge base article at http://kb.vmware.com/kb/2075011.

Index

A

artifact management, connecting **27**
Artifactory repository, users **24**
Artifactory server
  configuring **21**
  disk partitioning **25**
  registering **27**
  setting up password **19**

C

catalog items, publishing **25**
certificate chains, order **10**
chained certificates, order **10**
checklist, installing **11**
custom task **30**
custom workflow **30**

D

deleting, identity stores **21**

E

Encryption.key file, setting permissions **35**
endpoints, registering **27**
entitlements, users and groups **23**

F

failed installation, logs **33**

G

gating rule **31**
gating rule workflow **31**
glossary **5**
groups, creating custom groups **23**

I

identity stores
  adding **21**
  deleting **21**
Identity stores, troubleshooting **37**
identity manager, fails to start **36**
identity store
  configuring **21**
  domain requirements **9**
installation
  configuring **33**
  DNS and host name resolution **8**
  minimal installation overview **15**
  preparation **8**
  troubleshooting **33**
  vRealize Automation appliance **15**
Installation, using the management console **14**
installation preparation, time synchronization **11**
installation requirements
  credentials **9**
  deployment environments **8**
  hardware **8**
  operating system **8**
  port requirements **8**
  security **10**
  users **9**
  virtual machine **8**
Installation Wizard, overview **12**
installing, worksheet **12**
intended audience **5**

J

Jenkins, registering endpoint **28**

L

license, applying to appliance **19**
Log in errors, troubleshooting **37**
logs, locations **33**
Logs
  IaaS **33**
  troubleshooting **33**

M

Minimal deployments, install with installation wizard **13**
multiple users, creating **24**

N

NFS share, adding **25**

O

overview, installing **7**

P

password, restrictions **8**
PEM files, command for extracting **10**
plug-in, registering **27**
publishing, service blueprints **25**

R

release pipeline, registering endpoint **28**
roles
  assigning to custom groups **23**

assigning user roles **22**
managing user roles **21**
RSA private keys, command for extracting **10**

S

security
certificates **10**
passphrase **10**
service blueprints, publishing **25**
SSL certificates, extracting **10**
support bundle, creating **34**
System error message **35**

T

tenants
configuring **21**
troubleshooting ID stores **37**
troubleshooting login **37**
TFS, registering endpoint **31**
time synchronize, servers **16**
troubleshooting
blank pages appearing **35**
log locations **33**

U

users
granting user access **22**
managing **21**
users and groups, managing entitlements **23**

V

vRealize Appliance
configuring **17**
deploying **12, 15**
vRealize Automation, registering endpoint **29**
vRealize Automation appliances, troubleshooting **35**
vRealize Realize Automation appliance **15**