Administering vRealize Automation

21 July 2021
vRealize Automation 8.2

vmware®

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

https://docs.vmware.com/

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

Contents

Administering vRealize Automation

1

This guide describes how to monitor and manage critical infrastructure and user management aspects of a vRealize Automation deployment.

The tasks described herein are vital to keeping a vRealize Automation deployment operating appropriately. These tasks include user and group management, and monitoring system logs.

In addition, it describes how to configure and manage multi-organization deployments.

While some vRealize Automation administration tasks are completed from within vRealize Automation, others require the use of related products such as vRealize Suite Lifecycle Manager and Workspace ONE Access. Users should familiarize themselves with these products and their functionality before completing applicable tasks.

For example, for information about backup, restore, and disaster recovery, see the **Backup and Restore, and Disaster Recovery > 2019** section of vRealize Suite product documentation.

Note Disaster recovery is supported in vRealize Automation 8.0.1 and later.

For information about working with vRealize Suite Lifecycle Manager installation, upgrade, and management, see Lifecycle Manager product documentation.

Administering Users and Groups in vRealize Automation

2

vRealize Automation uses VMware Workspace ONE Access, the VMware supplied identity management application to import and manage users and groups. After users and groups are imported or created, you can manage the role assignments for single tenant deployments using the Identity & Access Management page.

vRealize Automation is installed using VMware Lifecycle Manager (vRSLCM or LCM). When installing vRealize Automation you must import an existing Workspace ONE Access instance, or deploy a new one to support identity management. These two scenarios define your management options.

- If you deploy a new Workspace ONE Access instance, you can manage users and groups via LCM. During installation, you can set up an Active Directory connection using Workspace ONE Access. Alternatively, you can view and edit some aspects of users and groups within vRealize Automation using the Identity & Access Management page as described herein.
- If you use an existing Workspace ONE Access instance, you import it for use with vRealize Automation via LCM during installation. In this case, you can continue to use Workspace ONE Access to manage users and groups, or you can use the management functions in LCM.

See Logging in to tenants and adding users in vRealize Automation for more information about managing users under a multi-organization deployment.

vRealize Automation users must be assigned roles. Roles define access to features within the application. When vRealize Automation is installed with a Workspace ONE Access instance, a default organization is created and the installer is assigned the Organization Owner role. All other vRealize Automation roles are assigned by the Organization Owner.

There are three types of roles in vRealize Automation: organization roles, service roles, and project roles. For vRealize Automation Cloud Assembly, Service Broker and Code Stream, typically, user level roles can use resources, while admin level roles are required to create and configure resources. Organizational roles define permissions within the tenant; organizational owners have admin level permissions while organizational members have user level permissions. Organization owners can add and manage other users.

Organization Roles	Service Roles
■ Organization Owner ■ Organization Member	■ Cloud Assembly Administrator ■ Cloud Assembly User ■ Cloud Assembly Viewer ■ Service Broker Administrator ■ Service Broker User ■ Service Broker Viewer ■ Code Stream Administrator ■ Code Stream User ■ Code Stream Viewer

In addition, there are two main project level roles not shown in the table: Project Administrator, and Project User. These roles are assigned ad hoc on a per project basis with Cloud Assembly. These roles are somewhat fluid. The same user can be an administrator on one project and a user on another project. For more information, see What are the vRealize Automation user roles.

For more information about working with LCM and Workspace ONE Access, see User Management with VMware Identity Manager.

This chapter includes the following topics:

- How do I enable Active Directory groups in vRealize Automation for projects
- How do I remove users in vRealize Automation
- How do I edit user roles in vRealize Automation
- How do I edit group role assignments in vRealize Automation
- What are the vRealize Automation user roles

How do I enable Active Directory groups in vRealize Automation for projects

If a group is not available on the Add Groups page when you are adding users to projects, check the Identity & Access Management page and add the group if it is available. If the group is not listed on the Identity & Access Management page in vRealize Automation, the group may not be synchronized in your Workspace One Access instance. You can verify that it has been synchronized and then use this procedure to add the group as shown herein.

To add members of an Active Directory group to a project, you must ensure that the group is synchronized with your Workspace One Access instance and that the group is added to the organization.

Prerequisites

If the groups are not synchronized, they are not available when you try to add them to a project. Verify that you synchronized your Active Directory groups with your Lifecycle Manager instance.

Procedure

1. Log in to vRealize Automation as a user from the same Active Directory domain that you are adding. For example, @mycompany.com
2. In Cloud Assembly, click Identity & Access Management in the header right navigation.
3. Click **Enterprise Groups**, and then click **Assign Roles**.
4. Use the search function to find the group that you are adding and select it.
5. Assign an organization role.

   At a minimum, the group must have an Organization Member role. SeeWhat are the Cloud Assembly user roles for more information.
6. Click **Add Service Access**, add one or more services, and select a role for each.
7. Click **Assign**.

Results

You can now add the Active Directory group to a project.

How do I remove users in vRealize Automation

You can remove users as needed in vRealize Automation.

All users are listed by default and you cannot add users with the Identity and Access Management page. You can delete users.

Procedure

1. Select the Active Users tab on the Identity & Access Management page.
2. Locate and select the users that you want to delete.
3. Click **Remove Users**.

Results

The selected users are removed.

How do I edit user roles in vRealize Automation

You can edit roles assigned to Workspace One Access users that have been imported into vRealize Automation.

Prerequisites

Procedure

1. In Cloud Assembly, click Identity & Access Management in the header right navigation.

2 Select the desired user on the Active Users tab and click **Edit Roles**.

3 You can edit the organization and service roles for the user.

- Select the drop down beside the Assign Organization Roles heading to change the user's relationship with the organization.
- Click Add Service Access to add new service roles for the user.
- To remove user roles, click the X beside the applicable service.

4 Click **Save**.

Results

The user role assignment is updated as specified.

How do I edit group role assignments in vRealize Automation

You can edit role assignments for groups in vRealize Automation

Prerequisites

Users and groups have been imported from a valid vIDM instance that is associated with your vRealize Automation deployment.

Procedure

1 In Cloud Assembly, click Identity & Access Management in the header right navigation.

2 Select the Enterprise Groups tab.

3 Type the name of the group for which you want to edit role assignments in the search field.

4 Edit the role assignments for the selected group. You have two options.

- Assign Organization Roles
- Assign Service Roles

5 Click **Assign**.

Results

Role assignments are updated as specified.

What are the vRealize Automation user roles

As a organization owner, you can assign users organization roles and service roles. The roles determine what the users can do or see. Then, in the services, the service administrator can assign project roles. To determine the role that you want to assign, evaluate the tasks in the following tables.

Cloud Assembly Service Roles

The vRealize Automation Cloud Assembly service roles determine what you can see and do in vRealize Automation Cloud Assembly. These service roles are defined in the console by an organization owner.

Table 2-1. vRealize Automation Cloud Assembly Service Role Descriptions

Role	Description
Cloud Assembly Administrator	A user who has read and write access to the entire user interface and API resources. This is the only user role that can see and do everything, including add cloud accounts, create new projects, and assign a project administrator.
Cloud Assembly User	A user who does not have the Cloud Assembly Administrator role. In a vRealize Automation Cloud Assembly project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Cloud Assembly Viewer	A user who has read access to see information but cannot create, update, or delete values. This is a read-only role across all projects. Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

In addition to the service roles, vRealize Automation Cloud Assembly has project roles. Any project is available in all of the services.

The project roles are defined in vRealize Automation Cloud Assembly and can vary between projects.

In the following tables, which tells you what the different service and project roles can see and do, remember that the service administrators have full permission on all areas of the user interface.

The descriptions of project roles will help you decide what permissions to give your users.

- Project administrators leverage the infrastructure that is created by the service administrator to ensure that their project members have the resources they need for their development work.
- Project members work within their projects to design and deploy cloud templates.
- Project viewers are restricted to read-only access, except in a few cases where they can do non-destructive things like download cloud templates.

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Access Cloud Assembly						
Console	In the vRA console, you can see and open Cloud Assembly	Yes	Yes	Yes	Yes	Yes
Infrastructure						
	See and open the Infrastructure tab	Yes	Yes	Yes	Yes	Yes
Configure - Projects	Create projects	Yes				
	Update, or delete values from project summary, users, provisioning, Kubernetes, integrations, and test project configurations.	Yes		Yes. Your projects		
	Add users and assign roles in projects.	Yes		Yes. Your projects.		
	View projects	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Configure - Cloud Zones	Create, update, or delete cloud zones	Yes				
	View cloud zones	Yes	Yes			
Configure - Kubernetes Zones	Create, update, or delete Kubernetes zones	Yes				
	View Kubernetes zones	Yes	Yes			
Configure - Flavors	Create, update, or delete flavors	Yes				
	View flavors	Yes	Yes			
Configure - Image Mappings	Create, update, or delete image mappings	Yes				

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View image mappings	Yes	Yes			
Configure - Network Profiles	Create, update, or delete network profiles	Yes				
	View image network profiles	Yes	Yes			
Configure - Storage Profiles	Create, update, or delete storage profiles	Yes				
	View image storage profiles	Yes	Yes			
Configure - Pricing Cards	Create, update, or delete pricing cards	Yes				
	View the pricing cards	Yes	Yes			
Configure - Tags	Create, update, or delete tags	Yes				
	View tags	Yes	Yes			
Resources - Compute	Add tags to discovered compute resources	Yes				
	View discovered compute resources	Yes	Yes			
Resources - Networks	Modify network tags, IP ranges, IP addresses	Yes				
	View discovered network resources	Yes	Yes			
Resources - Security	Add tags to discovered security groups	Yes				
	View discovered security groups	Yes	Yes			
Resources - Storage	Add tags to discovered storage	Yes				
	View storage	Yes	Yes			

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Resources - Machines	Add and delete machines	Yes				
	View machines	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Resources - Volumes	Delete discovered storage volumes	Yes				
	View discovered storage volumes	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects.
Resources - Kubernetes	Deploy or add Kubernetes clusters, and create or add namespaces	Yes				
	View Kubernetes clusters and namespaces	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Activity - Requests	Delete deployment request records	Yes				
	View deployment request records	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Activity - Event Logs	View event logs	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Connections - Cloud Accounts	Create, update, or delete cloud accounts	Yes				
	View cloud accounts	Yes	Yes			
Connections - Integrations	Create, update, or delete integrations	Yes				
	View integrations	Yes	Yes			
Onboarding	Create, update, or delete onboarding plans	Yes				
	View onboarding plans	Yes	Yes			Yes. Your projects
Marketplace						
	See and open the Marketplace tab	Yes	Yes			

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	Use the downloaded cloud templates on the Design tab	Yes		Yes. If associated with your projects.	Yes. If associated with your projects.	
Marketplace - Cloud Templates	Download a cloud template	Yes				
	View the cloud templates	Yes	Yes			
Marketplace - Images	Download images	Yes				
	View images	Yes	Yes			
Marketplace - Downloads	View the log of all downloaded items	Yes	Yes			
Extensibility						
	See and open the Extensibility tab	Yes	Yes			Yes
Events	View extensibility events	Yes	Yes			
Subscriptions	Create, update, or delete extensibility subscriptions	Yes				
	Deactivate subscriptions	Yes				
	View subscriptions	Yes	Yes			
Library - Event topics	View event topics	Yes	Yes			
Library - Actions	Create, update, or delete extensibility actions	Yes				
	View extensibility actions	Yes	Yes			
Library - Workflows	View extensibility workflows	Yes	Yes			
Activity - Action Runs	Cancel or delete extensibility action runs	Yes				

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View extensibility action runs	Yes	Yes			Yes. Your projects
Activity - Workflow Runs	View extensibility workflow runs	Yes	Yes			
Design						
Design	Open the Design tab and see a list of cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Cloud Templates	Create, update, and delete cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	View cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Download cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Upload cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Deploy cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Version and restore cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Release cloud templates to the catalog	Yes		Yes. Your projects	Yes. Your projects	
Custom Resources	Create, update or delete custom resources	Yes				
	View custom resources	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Custom Actions	Create, update, or delete custom actions	Yes				
	View custom actions	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Deployments						
	See and open the Deployments tab	Yes	Yes	Yes	Yes	Yes

Table 2-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View deployments, including deployment details, deployment history, and troubleshooting information.	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Run day 2 actions on deployments based on policies.	Yes		Yes. Your projects	Yes. Your projects	

Service Broker Service Roles

The vRealize Automation Service Broker service roles determine what you can see and do in vRealize Automation Service Broker. These service roles are defined in the console by an organization owner.

Table 2-3. Service Broker Service Role Descriptions

Role	Description
Service Broker Administrator	Must have read and write access to the entire user interface and API resources. This is the only user role that can perform all tasks, including creating a new project and assigning a project administrator.
Service Broker User	Any user who does not have the vRealize Automation Service Broker Administrator role. In a vRealize Automation Service Broker project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Service Broker Viewer	A user who has read access to see information but cannot create, update, or delete values. Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

In addition to the service roles, vRealize Automation Service Broker has project roles. Any project is available in all of the services.

The project roles are defined in vRealize Automation Service Broker and can vary between projects.

In the following tables, which tells you what the different service and project roles can see and do, remember that the service administrators have full permission on all areas of the user interface.

Use the following descriptions of project roles will help you as you decide what permissions to give your users.

- Project administrators leverage the infrastructure that is created by the service administrator to ensure that their project members have the resources they need for their development work.
- Project members work within their projects to design and deploy cloud templates.
- Project viewers are restricted to read-only access.

Table 2-4. Service Broker Service Roles and Project Roles

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Access Service Broker						
Console	In the console, you can see and open Service Broker	Yes	Yes	Yes	Yes	Yes
Infrastructure						
	See and open the Infrastructure tab	Yes	Yes			
Configure - Projects	Create projects	Yes				
	Update, or delete values from project summary, users, provisioning, Kubernetes, and integrations	Yes				
	View projects	Yes	Yes			
Configure - Cloud Zones	Create, update, or delete cloud zones	Yes				
	View cloud zones	Yes	Yes			
Configure - Kubernetes Zones	Create, update, or delete Kubernetes zones	Yes				

Table 2-4. Service Broker Service Roles and Project Roles (continued)

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View Kubernetes zones	Yes	Yes			
Connections - Cloud Accounts	Create, update, or delete cloud accounts	Yes				
	View cloud accounts	Yes	Yes			
Connections - Integrations	Create, update, or delete integrations	Yes				
	View integrations	Yes	Yes			
Activity - Requests	Delete deployment request records	Yes				
	View deployment request records	Yes				
Activity - Event Logs	View event logs	Yes				
Content and Policies						
	See and open the Content and Policies tab	Yes	Yes			
Content Sources	Create, update, or delete content sources	Yes				
	View content sources	Yes	Yes			
Content Sharing	Add or remove shared content	Yes				
	View shared content	Yes	Yes			
Content	Customize form and configure item	Yes				
	View content	Yes	Yes			
Policies - Definitions	Create, update, or delete policy definitions	Yes				
	View policy definitions	Yes	Yes			
Policies - Enforcement	View enforcement log	Yes	Yes			

Table 2-4. Service Broker Service Roles and Project Roles (continued)

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Notifications - Email Server	Configure an email server	Yes				
Catalog						
	See and open the Catalog tab	Yes	Yes	Yes	Yes	Yes
	View available catalog items	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Request a catalog item	Yes		Yes. Your projects	Yes. Your projects	
Deployments						
	See and open the Deployments tab	Yes	Yes	Yes.	Yes	Yes
	View deployments, including deployment details, deployment history, and troubleshooting information.	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Run day 2 actions on deployments based on policies	Yes		Yes. Your projects	Yes. Your projects	
Approvals						
	See and open the Approvals tab	Yes	Yes	Yes	Yes	Yes
	Respond to approval requests	Yes		Service Broker user role only	Service Broker user role only	Service Broker user role only

Maintaining your vRealize Automation appliance

3

As a system administrator, you might need to perform various tasks to ensure the proper functioning of your installed vRealize Automation application.

If you are just getting started with vRealize Automation, these are not required tasks. Knowing how to perform these tasks is useful if you need to resolve performance or product behavior issues.

This chapter includes the following topics:

Starting and stopping vRealize Automation

Observe the proper procedures when starting or shutting down vRealize Automation.

The recommended manner to shut down and start vRealize Automation components is to use the Power OFF and ON functionality provided in **Lifecycle Operations > Environments** section of vRealize Suite Lifecycle Manager. The following procedures outline manual methods to shut down and start vRealize Automation components in case vRealize Suite Lifecycle Manager is not available for some reason.

Shut down vRealize Automation

To preserve data integrity, shut down the vRealize Automation services before powering off the virtual appliances. Using SSH or VMRC, you can shut down or start all nodes from any individual appliance.

Note Avoid using `vracli reset vidm` commands if at all possible. This command resets all configurations of Workspace One Access and breaks the association between users and provisioned resources.

1 Log in to the console of any vRealize Automation appliance using either SSH or VMRC.

2 To shut down the vRealize Automation services on all cluster nodes, Run the following set of commands.

Note If you copy any of these commands to run and they fail, paste them into notepad first, and then copy them again before running them. This procedure strips out any hidden characters and other artifacts that might exist in the documentation source.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

3 Shut down the vRealize Automation appliances.

Your vRealize Automation deployment is now shut down.

Start vRealize Automation

Following an unplanned shutdown, a controlled shutdown, or a recovery procedure, you must restart vRealize Automation components in a specific order. vRLCM is a non-critical component, so you can start it at any time. VMware Workspace ONE Access, formerly VMware Identity Management, components must be started before you start vRealize Automation.

Note Verify that applicable load balancers are running before starting vRealize Automation components.

1 Power on all vRealize Automation appliances and wait for them to start.

2 Log into the console for any appliance using SSH or VMRC and run the following command to restore the services on all nodes.

```
/opt/scripts/deploy.sh
```

3 Verify that all services are up and running with the following command.

```
kubectl get pods --all-namespaces
```

Note You should see three instances of every service, with a status of either Running or Completed.

When all services are listed as Running or Completed, vRealize Automation is ready to use.

Restart vRealize Automation

You can restart all vRealize Automation services centrally from any of the appliances in your cluster. Follow the preceding instructions to shut down vRealize Automation, and then use the instructions to start vRealize Automation. Before restarting vRealize Automation, verify that all applicable load balancer and VMware Workspace ONE Access components are running.

When all services are listed as Running or Completed, then vRealize Automation is ready to use.

Run the following command to verify that all services are running:

```
kubectl -n prelude get pods
```

Scale out vRealize Automation from one to three nodes

As needs expand, you can scale out a vRealize Automation deployment from one node to three nodes.

You must use features of vRealize Suite Lifecycle Manager to complete many steps of this procedure. For information about working with vRealize Suite Lifecycle Manager installation, upgrade, and management, see Lifecycle Manager product documentation.

If you are using a three node clustered deployment, vRealize Automation can typically withstand the failure of one node and still function. The failure of two nodes in a three node cluster will render vRealize Automation non-functional.

Prerequisites

This procedure assumes that you already have a functioning single node vRealize Automation deployment.

Procedure

1 Shut down all vRealize Automation appliances.

To shut down the vRealize Automation services on all cluster nodes, run the following set of commands.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

Now you can shut down the vRealize Automation appliances.

2 Take a deployment snapshot.

Use the Create Snapshot option in vRealize Suite Lifecycle Manager **Lifecycle Operations > Environments > vRA > View Details**.

Note Online snapshots, taken without shutting down vRealize Automation nodes are supported from 8.0.1. For vRealize Automation 8.0 environments, you must stop vRealize Automation nodes first.

3 Power on the vRealize Automation appliance and bring up all containers.

4 Using the Locker functionality located at **LCM > Locker > Certificates** in vRealize Suite Lifecycle Manager, generate or import vRealize Automation certificates for all components including vRealize Suite Lifecycle Manager node FQDNs and the vRealize Automation Load Balancer fully qualified domain name.

Add the names of all three appliances in the Subject Alternative Names.

5 Import the new certificate into vRealize Suite Lifecycle Manager.

6 Replace the existing vRealize Suite Lifecycle Manager certificate with the one generated in the previous step using the LCM **Lifecycle Operations > Environments > vRA > View Details** Replace Certificate option.

7 Scale out vRealize Automation to three nodes using the Add Components selection in **LCM > Lifecycle Operations > Environments > vRA > View Details**.

Results

vRealize Automation has been scaled to a three node deployment.

Replacing a vRealize Automation appliance node

When a vRealize Automation appliance in a multiple-node, high availability (HA) configuration has failed, you might need to replace the faulty node.

Caution Before proceeding, VMware recommends that you contact technical support to troubleshoot the HA issue and verify that the problem is isolated to one node.

If technical support determines that you need to replace the node, take the following steps.

1 In vCenter, take backup snapshots of every appliance in the HA configuration.

In the backup snapshots, don't include virtual machine memory.

2 Shut down the faulty node.

3 Make note of the faulty node vRealize Automation software build number, and network settings.

Note the FQDN, IP address, gateway, DNS servers, and especially MAC address. Later, you assign the same values to the replacement node.

4 The primary database node must be one of the healthy nodes. Follow these steps:

a Log in as root to the command line of a healthy node.

b Find the name of the primary database node by running the following command.

```
vracli status | grep primary -B 1
```

The result should be similar to this example, where postgres-1 is the primary database node.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

c Verify that the primary database node is healthy by running the following command.

```
kubectl -n prelude get pods -o wide | grep postgres
```

The result should be similar to this example, where postgres-1 is in the list as running and healthy.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Important If the primary database node is faulty, contact technical support instead of proceeding.

5 From the root command line of the healthy node, remove the faulty node.

```
vracli cluster remove faulty-node-FQDN
```

6 Use vCenter to deploy a new, replacement vRealize Automation node.

Deploy the same vRealize Automation software build number, and apply the network settings from the faulty node. Include the FQDN, IP address, gateway, DNS servers, and especially MAC address that you noted earlier.

7 Power on the replacement node.

8 Log in as root to the command line of the replacement node.

9 Verify that the initial boot sequence has finished by running the following command.

```
vracli status first-boot
```

Look for a `First boot complete` message.

10 From the replacement node, join the vRealize Automation cluster.

```
vracli cluster join primary-DB-node-FQDN
```

11 Log in as root to the command line of the primary database node.

12 Deploy the repaired cluster by running the following script.

```
/opt/scripts/deploy.sh
```

Increase vRealize Automation appliance disk space

You might need to increase vRealize Automation appliance disk space for purposes such as log file storage.

Procedure

1 Use vSphere to expand the VMDK on the vRealize Automation appliance.

2 Log in to the command line of the vRealize Automation appliance as a root user.

3 From the command prompt, run the following vRealize Automation command:

```
vracli disk-mgr resize
```

If vRealize Automation resizing fails, see Knowledge Base article 79925.

Update the DNS assignment for vRealize Automation

An administrator can update the DNS assignments for vRealize Automation.

Procedure

1 Log in to the console for any vRealize Automation appliance using either SSH or VMRC.

2 To shut down the vRealize Automation services on all cluster nodes, run the following set of commands.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

3 Log in to vCenter and shut down all vRealize Automation nodes using the `Shut Down Guest OS` command.

4 Update the OVF DNS property for each vRealize Automation node.

   a Navigate to the vRealize Automation node from the vCenter inventory.

   b Select the Configure tab and expand Settings.

   c Select vApp options.

   d In the list of OVF properties locate and select `vami.DNS.vRealize_Automation`.

   e Click **Set value** and enter the new DNS entries in the Property value text box.

   f Click **OK**.

5 Start all vRealize Automation nodes and wait for them to start completely, which will be indicated by a blue screen on the console.

6 Restart the vRealize Automation nodes again and wait for them to start completely.

7 Log in to each vRealize Automation node with SSH and verify that the new DNS servers are listed in `/etc/resolve.conf`.

8 On one of the vRealize Automation nodes, run the following command to start the vRealize Automation services: `/opt/scripts/deploy.sh`

Results

The vRealize Automation DNS settings are changed as specified.

How do I enable time synchronization of vRealize Automation

You can enable time synchronization on your vRealize Automation deployment by using the vRealize Automation Appliance command line.

You can configure time synchronization for your standalone or clustered vRealize Automation deployment by using the Network Time Protocol (NTP) networking protocol. vRealize Automation supports two mutually exclusive NTP configurations:

NTP configuration	Description
ESXi	You can use this configuration when the ESXi server hosting the vRealize Automation Appliance is synchronized with an NTP server. If you are using a clustered deployment, all ESXi hosts must be synchronized with an NTP server. **Note** You can experience clock drift if your vRealize Automation deployment is migrated to a ESXi host that is not synchronized to an NTP server. For more information on configuring NTP for ESXi, see KB article 57147 Configuring Network Time Protocol (NTP) on an ESXi host using the vSphere Web Client.
systemd	This configuration uses the systemd-timesyncd daemon to synchronize the clocks of your vRealize Automation deployment. **Note** By default, the systemd-timesyncd daemon is enabled, but configured with no NTP servers. If the vRealize Automation Appliance uses a dynamic IP configuration, the appliance can use any NTP servers received by the DHCP protocol.

Procedure

1 Log in to the vRealize Automation Appliance command line as **root**.

2 Enable NTP with ESXi.

   a Run the `vracli ntp esxi` command.

   b Run the `vracli ntp apply` command.

      The ESXi NTP configuration is applied to the vRealize Automation deployment.

3 Enable NTP with systemd.

   a Run the `vracli ntp systemd --set` *`FQDN_or_IP_of_systemd_server`* command.

      Note You can add multiple systemd NTP servers by separating their network addresses with a comma.

   b Run the `vracli ntp apply` command.

      The systemd NTP configuration is applied to the vRealize Automation deployment.

4 (Optional) To confirm the status of the NTP configuration, run the `vracli ntp status` command.

   The NTP configuration can fail if there is a time difference of more than 10 minutes between the NTP server and the vRealize Automation deployment. To resolve this issue, reboot the vRealize Automation Appliance that is synchronized with the NTP server.

How do I reset the root password for vRealize Automation

You can reset a lost or forgotten vRealize Automation root password.

In this procedure, you use a command line window on the host vCenter appliance to reset your organization's vRealize Automation root password.

Prerequisites

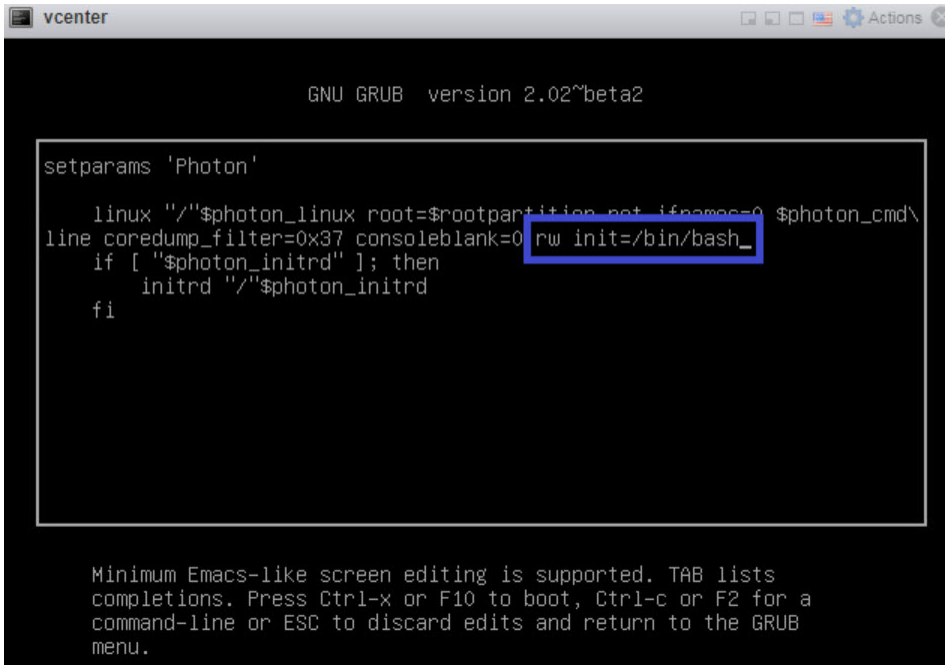
This process is for vRealize Automation administrators and requires the credentials needed to access the host vCenter appliance.

Procedure

1 Shut down and start up vRealize Automation by using the procedure described in Starting and stopping vRealize Automation.

2 When the Photon operating system command line window appears, enter `e` and press the **Enter** key to open the `GNU GRUB` boot menu editor.

3 In the `GNU GRUB` editor, enter `rw init=/bin/bash` at the end of the line that begins with `linux "/" $photon_linux root=rootpartition` as shown below:



4 Click the **F10** key to push your change and restart vRealize Automation.

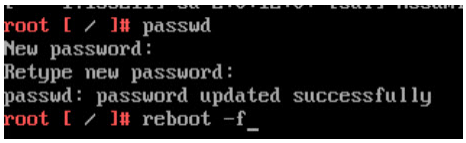
5 Wait for vRealize Automation to restart.

6 At the `root [/]#` prompt, enter `passwd` and press the **Enter** key.

7 At the `New password:` prompt, enter your new password and press the **Enter** key.

8 At the `Retype new password:` prompt, reenter your new password and press the **Enter** key.

9 At the `root [/]#` prompt, enter `reboot -f` and press the **Enter** key to complete the root password reset process.



What to do next

As a vRealize Automation administrator, you can now log in to vRealize Automation with the new root password.

Using multi-organization tenant configurations in vRealize Automation

4

vRealize Automation enables customer IT providers, to set up multiple tenants, or organizations, within each deployment. Providers can set up multiple tenant organizations and allocate infrastructure within each deployment. Providers can also manage users for tenants. Each tenant manages its own projects, resources, and deployments.

In a vRealize Automation multi-organization configuration, providers can create multiple organizations, and each tenant organization uses its own projects, resources and deployments. While providers cannot manage tenant infrastructure remotely, they can log in to tenants and manage infrastructure within their tenants.

Multi-tenancy relies on coordination and configuration of three different VMware products as outlined below:

- Workspace ONE Access - This product provides the infrastructure support for multi-tenancy and the Active Directory domain connections that provide user and group management within tenant organizations.
- vRealize Suite Lifecycle Manager - This product supports the creation and configuration of tenants for supported products, such as vRealize Automation. In addition, it provides some certificate management capabilities.
- vRealize Automation - Providers and users log in to vRealize Automation to access tenants in which they create and manage deployments.

When configuring multi-tenancy, users should be familiar with all three of these products and their associated documentation.

For more information about working with Lifecycle Manager and Workspace ONE Access, see User Management with VMware Identity Manager and Managing Users and Groups.

Administrators with vRealize Suite Lifecycle Manager privileges create and manage tenants using the Lifecycle Manager Tenanats page located under the Identity and Tenant Management service. Tenants are constructed using an Active Directory IWA or LDAP connection, and they are supported by the associated VMware Workspace ONE Access instance that is required for vRealize Automation deployments. See the associated documentation for information about using Lifecycle Manager.

When configuring multi-tenancy, you start with a base, or master tenant. This tenant is the default tenant that is created when the underlying Workspace ONE Access application is deployed. Other tenants, known as sub-tenants, can be based upon the master tenant. vRealize Automation currently supports up to 20 tenant organizations with the standard three node deployment.

When configuring vRealize Automation for multi-tenancy, you must first install the application in a single organization configuration, and then use Lifecycle Manager to set up a multi-organization configuration. A Workspace ONE Access deployment supports the management of tenants and the associated Actice Directory domain connections.

When multi-tenancy is initially configured, a provider administrator is designated in Lifecycle Manager. You can change this designation or add administrators later if desired. Under multit-organizartion configurations, vRealize Automation users and groups are managed primarily through Workspace ONE Access.

After organizations are created, authorized users can log in to their applications to create or work with projects and resources and create deployments. Administrators can manage user roles in vRealize Automation.

Setting up for a multi-organization configuration

You can enable a multi-organization deployment after completing a vRealize Automation installation. When setting up a multi-organization configuration, you must configure your external Workspace ONE Access for multi-tenancy use and then use Lifecycle manager to create and configure tenants. This applies to both new and existing deployments. As an initial step to setting up tenants, you must use Lifecycle Manager to set an alias for the master tenant that was created by default on Workspace ONE Access. Sub-tenants that you create based on this master tenant inherit the Active Directory domain configurations from this master tenant.

In Lifecycle Manager, you assign tenants to a product, such as vRealize Automation, and to a specific environment. When setting up a tenant, you must also designate a tenant administrator. By default, multi-tenancy is enabled based on tenant hostname. Users can elect to manually configure tenant name by DNS name. During this procedure you must set several flags to support multi-tenancy, and you must configure the load balancer as well.

If you use a clustered instance, both the Workspace ONE Access and vRealize Automation tenant based hostnames will point to the load balancer.

If your clustered vRealize Automation and Workspace ONE Access load balancers do not use wildcard certificates, then users must add tenant hostnames as SAN entries on the certificates. for every new tenant that is created.

You cannot delete tenants in vRealize Automation or in Lifecycle Manager. If you need to add tenants to an existing multi-tenancy deployment, you can do this using Lifecycle Manager, but it will necssitate downtime of three to four hours.

Hostnames and multi-tenancy

In prior versions of vRealize Automation, users accessed tenants with URLs that were based on directory path. In the current multi-tenancy implementation, users access tenants based on hostname.

Also, the hostname format that vRealize Automation users will use to access tenants differs from the format that is used to access tenants within Workspace ONE Access. For example, a valid hostname would look like the following: `tenant1.example.eng.vmware.com` as opposed to `vidm-node1.eng.vmware.com`.

Multi-tenancy and certificates

You must create certificates for all components involved in a multi-organization configuration. You will need one or more certificates for Workspace ONE Access, Lifecycle Manager, and vRealize Automation, depending on whether you are using a single node configuration or a clustered configuration.

When configuring certificates, you can use either wildcards with the SAN names or dedicated names. Using wildcards will simplify certificate management somewhat as certificates must be updated whenever you add new tenants. If your vRealize Automation and Workspace ONE Access load balancer do not use wildcard certificates, then you must add tenant hostnames as SAN entries on the certificates for every new tenant that is created. Also, if you use SAN, certificates must be updated manually if you add or delete hosts or change a hostname. You must also update DNS entries for tenants.

Note that Lifecyle Manager does not create separate certificates for each tenant. Instead it creates a single certificate with each tenant hostname listed. For basic configurations, the tenant's CNAME uses the following format: *tenantname.vrahostname.domain*. For high availablity configurations, the name uses the following format: *tenantname.vraLBhostname*.domain.

If you are using a clustered Workspace ONE Access configuration, note that Lifecycle Manager cannot update the load balancer certificate, so you must update it manaully. Also, if you need to re-register products or services that are external to Lifecycle Manager, this is a manual process.

This chapter includes the following topics:

- Set up multi-organization tenancy for vRealize Automation
- Logging in to tenants and adding users in vRealize Automation
- Using vRealize Orchestrator with vRealize Automation multi-organization deployments

Set up multi-organization tenancy for vRealize Automation

You can set up multi-organization tenancy for vRealize Automation using vRealize Suite Lifecycle Manager.

The following is a high level description of the procedure to set up multi-tenancy for vRealize Automation including configuring DNS and certificates. It focuses on a single node deployment but includes notes for a clustered configuration.

See https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/ for more information and a video demonstration of configuring a vRealize Automation multi-organization configuration.

Prerequisites

- Install and configure Workspace ONE Accessversion 3.3.2.
- Install and configure vRealize Suite Lifecycle Manager version 8.2.

Procedure

1 Create the required A and CNAME Type DNS records.

   - For your master tenant and each sub-tenant, you must create and apply a SAN certificate.
   - For single node deployments, the vRealize Automation FQDN points to the vRealize Automation appliance, and the Workspace ONE Access FQDN points to the Workspace ONE Access appliance.
   - For clustered deployments, both the Workspace ONE Access and vRealize Automation tenant-based FQDNs must point to their respective load balancers. Workspace ONE Access is configured with SSL Termination, so the certificate is applied on both the Workspace ONE Access cluster and load balancer. The vRealize Automation load balancer uses SSL passthrough, so the certificate is applied only on the vRealize Automation cluster.

   See Managing certificates and DNS configuration under single-node multi-organization deployments and Managing certificate and DNS configuration under clustered vRealize Automation deployments for more details.

2 Create or import the required multi-domain (SAN) certificates for both Workspace One 3.3.2 and vRA 8.2.

   You can create certificates in Lifecycle Manager using the Locker service that enables you to create certificates licenses, and passwords. Alternatively, you can use a CA server or some other mechanism to generate certificates.

   If you need to add or create additional tenants, you must recreate and apply your vRealize Automation and Workspace ONE Access tenants.

   After you create your certificates, you can apply them within Lifecycle Manager using the Lifecycle Operations feature. You must select the environment and product and then the Replace Certificate option on the righthand menu. Then you can select the product. When you replace a certificate, you must re-trust all associated products in your environment.

   You must wait for the certificate to be applied and all services to restart before proceeding to the next step.

See Managing certificates and DNS configuration under single-node multi-organization deployments and Managing certificate and DNS configuration under clustered vRealize Automation deployments for more details.

3 Apply the Workspace One SAN certificate on the Workspace ONE Access instance or cluster.

4 In vRealize Suite Lifecycle Manager, run the Enable Tenancy wizard to enable mult-tenancy and create an alias for the default master tenant.

   Enabling tenancy requires that you create an alias for the provider organization master tenant or default tenant. After you enable tenancy, you can access Workspace ONE Access via the master tenant FQDN.

   For example, if the existing Workspace ONE Access FQDN is `idm.example.local` and you create an alias of default-tenant, after tenancy is enabled, the Workspace ONE Access FQDN changes to `default-tenant.example.local`, and all clients communicating with Workspace ONE Access would now communicate through `default-tenant.example.local`.

5 Apply the vRealize Automation SAN certificates on the vRealize Automation instance or cluster.

   You can apply SAN certificates through the Lifecycle Manager Lifecycle Operations service. You need to view the details of the environment and then select Replace Certificates on the right menu. You must wait for the certificate replacement task to complete before adding tenants. As part of certificate replacement, vRealize Automation services will restart.

6 In Lifecycle Manager, run the Add Tenants wizard to configure the desired tenants.

   You add tenants using the Lifecycle Manager Tenant Management page located under Identity and Tenant Management. You can only add tenants for which you have previously configured certificates and DNS settings.

   When creating a tenant, you must designate a tenant administrator and you can select the Active Directory connections for this tenant. Available connections are based on those configured in your default or master tenant. You must also select the product or product instance to which the tenant will be associated.

What to do next

After you create tenants, you can use the Lifecycle Manager Tenant Management page located under Identity and Tenant Management to change or add tenant administrators, add Active Directory directories to the tenant and change product associations for the tenant.

You can also log in to your Workspace ONE Access instance to view and validate your tenant configuration.

Managing certificates and DNS configuration under single-node multi-organization deployments

Multi-organization tenancy vRealize Automation configurations rely on a coordinated configuration between several products, and you must ensure that DNS settings and certificates are configured correctly in order for your multi-organization tenancy configuration to function.

This multi-organization configuration assumes single node deployments for the following components:

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Also, it assumes that you are starting with a default tenant, which is your provider organization, and creating two sub-tenants, called tenant-1 and tenant-2.

You can create and apply certificates using the Locker service in vRealize Suite Lifecycle Manager or you can use another mechanism. Lifecycle manager also enables you to replace or re-trust certificates on vRealize Automation or Workspace ONE Access.

DNS Requirements

You must create both main A type records and CNAME type records for system components as described below.

- Create both main A type records for each system component and for each of the tenants that you will create when you enable multi-tenancy.
- Create multi-tenancy A type records for each of the tenants you will create as well as for the master tenant.
- Ccreate multi-tenancy CNAME type records for each of the tenants you will create, not including the master tenant.

Certificate requirements for single node multi-tenancy deployment

You must create two Subject Alternative Name (SAN) certificates, one for Workspace ONE Access and one for vRealize Automation.

- The vRealize Automation certificate lists the hostname of the vRealize Automation server and the names of the tenants you will create.
- The Workspace ONE Access certificate lists the hostname of the Workspace ONE Access server and the tenant names you are creating.

- If you use dedicated SAN names, certificates must be updated manually when you add or delete hosts or change a hostname. You must also update DNS entries for tenants. As an option to simplify configuration, you can use wildcards for the Workspace ONE Access and vRealize Automation certificates. For example, `*.example.com` and `*.vra.example.com`.

  Note vRealize Automation 8.x supports wildcard certificates only for DNS names that match the specifications in the Public Suffix list at https://publicsuffix.org. For example, `*.myorg.com` is a valid name while `*.myorg.local` is invalid.

Note that Lifecyle Manager does not create separate certificates for each tenant. Instead it creates a single certificate with each tenant hostname listed. For basic configurations, the tenant's CNAME uses the following format: *tenantname.vrahostname*.domain. For high availability configurations, the name uses the following format: *tenantname.vraLBhostname*.domain.

Summary

The following table summarizes DNS and certificate requirements for a single node Workspace ONE Access and single node vRealize Automation deployment.

DNS Requirements	SAN Certificate Requirements
`Main A Type Records` lcm.example.local WorkspaceOne.example.local vra.example.local	`Workspace One Certificate` Host Name: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
`Multi-tenancy A Type Records` default-tenant.example.local tenant-1.example.local tenant-2.example.local	
`Multi-Tenancy CNAME Type Records` tenant-1.vra.example.local tenant-2.vra.example.local	`vRealize Automation Certificate` Host Name: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Managing certificate and DNS configuration under clustered vRealize Automation deployments

You must coordinate the certificate and DNS configuration between all applicable components to set up a multi-organization clustered vRealize Automation deployment.

In a typical clustered configuration, there are three Workspace ONE Access appliances and three vRealize Automation appliances as well as a single Lifecycle Manager appliance.

This configuration assumes clustered deployments for the following components:

- Workspace ONE Access Identity Manager appliances:
  - idm1.example.local
  - idm2.example.local

    - idm3.example.local
    - idm-lb.example.local
- vRealize Automation appliances:
    - vra1.example.local
    - vra2.example.local
    - vra3.example.local
    - vra-lb.example.local
- Lifecycle Manager appliance

DNS Requirements

You must create both main A type records for each component and for each of the tenants that you will create when you enable multi-tenancy. In addition, you must create multi-tenancy CNAME type records for each of the tenants you will create, not including the master tenant. Finally, you must also create Main A Type records for the Workspace ONE Access and vRealize Automation load balancers.

- Create A type records for the three Workspace ONE Access appliances, and for the vRealize Automation appliances that point to their respective FQDNs.
- In addition, create A type records for the Workspace ONE Access load balancer and the vRealize Automation load balancer that point to their respective FQDNs.
- Create multi-tenancy A Type records for the default tenant and for tenant-1 and tenant-2 that point to the IP address of the Workspace ONE Access load balancer.
- Create CNAME records for tenant-1 and tenant-2 that point to the IP address of the vRealize Automation load balancer.

Subject Alternative Name (SAN) Certificate Requirements

You must create two Workspace ONE Access certificates, one that applies on the cluster appliances and one that applies on the load balancer. In addition, create a certificate that applies to the vRealize Automation appliances, the tenants you are creating, excluding the default tenant, and the load balancer.

- Create a certificate for the Workspace ONE Access appliances that list the FQDNs of the Workspace ONE Access appliances as well as the default tenant and other tenants you create. This certificate should include the IP addresses of the Workspace ONE Access appliances.
- As a best practice, create an SSL termination on the load balancer. To support this ternination, create a certificate for the Workspace ONE Access load balancer that lists the FQDN of the Workspace ONE Access load balancer as well as the default tenant and all other tenants you create. This certificate should include the IP address of the load balancer.

- You must create a certificate for vRealize Automation that lists the host names of the three vRealize Automation appliances as well as the related load balancer and the tenants you are creating. In addition, it should list the IP addresses of the three vRealize Automation appliances.
- As an option, to simplify configuration, you can use wildcards for the Workspace ONE Access and vRealize Automation certificates. For example, `*.example.com`, `*.vra.example.com`, and `*.vra-lb.example.com`.

  Note vRealize Automation 8.x supports wildcard certificates only for DNS names that match the specifications in the Public Suffix list at https://publicsuffix.org. For example, `*.myorg.com` is a valid name while `*.myorg.local` is invalid.

If you are using a clustered Workspace ONE Access configuration, note that Lifecycle Manager cannot update the load balancer certificates, so you must update them manaully. Also, if you need to re-register products or services that are external to Lifecycle Manager, this is a manual process.

Summary of DNS entries and certificates for a clustered multi-organization configuration

The following table outlines DNS and certificate requirements for a clustered Workspace ONE Access and clustered vRealize Automation multi-organization deployment.

DNS Requirements	SAN Certificate Requirements
`Main A Type Records` lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	`Workspace One Certificate` Host Name: WorkspaceOne.example.local, default-tenant,example.local, tenant-1.example.local, tenant-2.example.local
`Multi-Tenancy A Type Records` default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	`Workspace One LB Certificate (LB Terminated)` Host Name: WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
`Multi-Tenancy CNAME Type Records` tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.exmple.local	`vRealize Automation Certificate` Host Name: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local No certificate is required on the vRealize Automation load balancer as it uses SSL passthrough.

Logging in to tenants and adding users in vRealize Automation

After you have created tenants for vRealize Automation in Lifecycle Manager, you can log in to Workspace ONE Access to view your tenants and add users.

You can view tenants created for a vRealize Automation deployment by logging in to the associated Workspace ONE Access instance. The URL to use is `https://default-tenant name.domainname.local` or, for a non-clustered deployment, `https://idm.domainname.local` which will direct you back to the default tenant Workspace ONE Access URL.

You can validate specific tenants in Workspace ONE Access using the following URL: `https://tenant-1.domainname.local`. This URL opens a page that show the users for the specified tenant. You can click **Add User** to create additional users on an ad-hoc basis.

Authorized users can log in to the main provider organization in vRealize Automation using `https://vra.domainname.local`. This view provides access to all vRealize Automation related services.

Authorized users can log in to applicable tenants in vRealize Automation using `https://tenantname.vra.domainname.local`.

For more information about managing users in Workspace ONE Access, see Managing Users and Groups in Workspace ONE Access product documentation.

Adding local users

You can add local users to your deployment using the associated Workspace ONE Access instance. Local users are users that are not stored in any external identity provider.

Using vRealize Orchestrator with vRealize Automation multi-organization deployments

You can use vRealize Orchestrator with vRealize Automation multi-organization tenancy deployments.

The default tenant supports integration with the embedded vRealize Orchestrator integration out of the box. vRealize Orchestrator is available pre-configured on the Integrations page. Sub-tenants do not have any pre-registered vRealize Orchestrator integration. They do have several options to add vRealize Orchestrator integration.

- They can add integration with the embedded vRealize Orchestrator by navigating to Configure Authentication Provider in vRealize Orchestrator and connecting using the host address of the applicable vRealize Automation tenant. Then they can select **Infrastructure > Connections > Integrations** and add the embedded vRO as an integration.
- They can add an external vRealize Orchestrator instance that uses the multi-organization vRealize Automation as an Auth Provider.

Any vRealize Orchestrator instance that uses a vRealize Automation multi-organization deployment as an Auth Provider can be registered to any of the tenants by creating a new integration and providing the vRealize Orchestrator FQDN without providing any credentials.

Working with logs in vRealize Automation

5

You can use the supplied `vracli` command line utility to create and use logs in vRealize Automation.

You can use logs directly in vRealize Automation or you can instead forward all logs to vRealize Log Insight.

This chapter includes the following topics:

How do I work with logs and log bundles in vRealize Automation

Logs are generated automatically by the various services. You can generate log bundles in vRealize Automation. You can also configure your environment to automatically forward logs to vRealize Log Insight.

Information about how to use the `vracli` command line utility to generate log bundles is available by using the `--help` argument in the `vracli` command line (for example, `vracli log-bundle --help`).

For related information about using vRealize Log Insight, see How do I configure log forwarding to vRealize Log Insight.

Log bundle commands

You can create a log bundle to contain all the logs that are generated by the services that you run. A log bundle contains all your service logs and is needed for troubleshooting.

In a clustered environment (high availability mode), run the `vracli log-bundle` command on only one node. Logs are pulled from all nodes in the environment. However, in the event of a networking or other cluster issue, logs are pulled from as many nodes as can be reached. For example, if one node is disconnected in a cluster of three nodes, logs are only collected from the two healthy nodes. Output from the `vracli log-bundle` command contains information about any issues found and their workaround steps.

- To create a log bundle, SSH to any node and run the following `vracli` command:

  ```
  vracli log-bundle
  ```

- To change the timeout value for collecting logs from each node, run the following `vracli` command:

  ```
  vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
  ```

  For example, if your environment contains large log files, slow networking, or high CPU usage, you can set the timeout to greater than the 1000 second default value.

- To configure other options such as assembly timeout and buffer location, use the following `vracli` help command:

  ```
  vracli log-bundle --help
  ```

Log bundle structure

The log bundle is a timestamped tar file. The name of the bundle matches the patter `log-bundle-<date>T<time>.tar` file, for example `log-bundle-20200629T131312.tar`. Typically the log bundle contains logs from all nodes in the environment. In case of an error, it contains as many logs as possible. It minimally contains logs from the local node.

The log bundle consists of the following content:

- Environment file

  The environment file contains the output of various Kubernetes maintenance commands. It supplies information about current resource usage per nodes and per pods. It also contains cluster information and description of all available Kubernetes entities.

- Host logs and configuration

  The configuration of each host (for example its `/etc` directory) and the host-specific logs (for example `journald`) are collected in one directory for each cluster node or host. The name of the directory matches the hostname of the node. The internal contents of the directory match the file system of the host. The number of such directories matches the number of cluster nodes.

- Services logs

Logs of the running Kubernetes services are available in the `<hostname>/services-logs/<namespace>/<app-name>/<container-name>.log`. An example file name is `my-host-01/services-logs/prelude/vco-app/vco-server-app.log`.

- *hostname* is the hostname of the node on which the application container is or was running. Typically, there is one instance for each node for each service. For example, 3 nodes = 3 instances.
- *namespace* is the Kubernetes namespace in which the application is or was deployed. For user-facing services, this value is `prelude`.
- *app-name* is the name of the Kubernetes application that produced the logs, for example `provisioning-service-app`.
- *container-name* is the name of the container that produced the logs. Some apps consist of multiple containers. For example, `vco-app` contains the `vco-server-app` and `vco-controlcenter-app` containers.

- (Legacy) Pod logs

  Prior to the logging architecture changes made in vRealize Automation 8.2, services logs (described in the previous bullet) were located in each pod's directory in the log bundle. While you can continue to generate pod logs in the bundle by using the `vracli log-bundle --include-legacy-pod-logs` command line, doing so is not advised as all log information already resides in each services' logs. Including pod logs can unnecessarily increase the time and space required to generate the log bundle.

How do I configure log forwarding to vRealize Log Insight

You can forward logs from vRealize Automation to vRealize Log Insight to take advantage of more robust log analysis and report generation.

vRealize Automation is bundled with a fluentd-based logging agent. The agent collects and stores logs so that they can be included in a log bundle and examined later. You can configure the agent to forward a copy of the logs to a vRealize Log Insight server by using the vRealize Log Insight REST API. The API allows other programs to communicate with vRealize Log Insight.

For more information about vRealize Log Insight, including documentation for the vRealize Log Insight REST API, see vRealize Log Insight documentation.

Configure the logging agent to continuously forward vRealize Automation logs to vRealize Log Insight by using the supplied `vracli` command line utility.

All log lines are tagged with a host name and environment tag and can be examined in vRealize Log Insight. In a high availability (HA) environment, logs are tagged with different host names, depending on the node that they originated on. The environment tag is configurable by using the `--environment ENV` option as described below in the *Configure or update integration of vRealize Log Insight* section. In an HA environment, the environment tag has the same value for all log lines, regardless of the node they originated on.

Information about how to use the `vracli` command line utility is available by using the `--help` argument in the `vracli` command line. For example: `vracli vrli --help`.

Check existing configuration of vRealize Log Insight

`Command`

`vracli vrli`

`Arguments`

There are no command line arguments.

`Output`

The current configuration for vRealize Log Insight integration is output in JSON format.

`Exit codes`

The following exit codes are possible:

- 0 - Integration with vRealize Log Insight is configured.
- 1 - An exception occurred as part of command execution. Examine the error message for details.
- 61 (ENODATA) - Integration with vRealize Log Insight is not configured. Examine the error message for details.

`Example - check integration configuration`

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
    "agentId": "0",
    "environment": "prod",
    "host": "my-vrli.local",
    "port": 9543,
    "scheme": "https",
    "sslVerify": false
}
```

Configure or update integration of vRealize Log Insight

`Command`

`vracli vrli set [options] FQDN_OR_URL`

Note After you run the command, it can take up to 2 minutes for the logging agent to apply your specified configuration.

`Arguments`

- FQDN_OR_URL

  Specifies the FQDN or IP address of the vRealize Log Insight server to use for posting logs. Port 9543 and https are used by default. If any of these settings must be changed, you can use a URL instead.

  Note You can set a different host scheme (default is https) and port (default for https is 9543, default for http is 9000) to use for sending the logs, as shown in the following samples:

  ```
  vracli vrli set some-host
  vracli vrli set some-host:9543
  vracli vrli set http://some-host:9000
  ```

  Ports 9543 for https and 9000 for http are used by the vRealize Log Insight ingestion REST API as described in the *Administering vRealize Log Insight* topic *Ports and External Interfaces* in vRealize Log Insight documentation.

- Options
  - --agent-id SOME_ID

    Sets the id of the logging agent for this appliance. The default is `0`. Used to identify the agent when posting logs to vRealize Log Insight by using the vRealize Log Insight REST API.

  - --environment ENV

    Sets an identifier for the current environment. It will be available in vRealize Log Insight logs as a tag for each log entry. The default is `prod`.

  - --ca-file /path/to/server-ca.crt

    Specifies a file that contains the certificate of the certificate authority (CA) that was used to sign the certificate of the vRealize Log Insight server. This forces the logging agent to trust the specified CA and enable it to verify the certificate of the vRealize Log Insight server if it was signed by an untrusted authority. The file may contain a whole certificate chain to verify the certificate. In the case of a self-signed certificate, pass the certificate itself.

  - --ca-cert CA_CERT

    Definition is identical to that of --ca-file as above, but instead passes the certificate (chain) inline as string.

  - --insecure

    Deactivates SSL verification of the server certificate. This forces the logging agent to accept any SSL certificate when posting logs.

- Advanced options
  - --request-max-size BYTES

Multiple log events are ingested with a single API call. This argument controls the maximum payload size, in bytes, for each request. Valid values are between 4000 and 4000000. The default value is 256000. For related information for allowed values, see vRealize Log Insight events ingestion in the vRealize Log Insight REST API documentation. Setting this value too low can cause logging events that are larger than the allowed size to be dropped.

- --request-timeout SECONDS

  A call to the API can hang for a number of reasons including problems with the remote, networking issues,and so on. This parameter controls the number of seconds wait for each operation to complete, such as opening a connection, writing data, or awaiting a response, before the call is recognized as failed. The value cannot be less than 1 second. The default is 30.

- --request-immediate-retries RETRIES

  Logs are buffered in aggregated chunks before they are sent to vRealize Log Insight (see --buffer-flush-thread-count below). If an API request fails, the log is retried immediately. The default number of immediate retries is 3. If none of the retries is successful, then the whole log chunk is rolled back and is retried again later.

- --buffer-flush-thread-count THREADS

  For better performance and to limit networking traffic, logs are buffered locally in chunks before they are flushed and sent to the log server. Each chunk contains logs from a single service. Depending on your environment, chunks can grow large and time-consuming to flush. This argument controls the number of chunks that can be flushed simultaneously. The default is 2.

Note When configuring integration over https, if the vRealize Log Insight server is configured to use an untrusted certificate such as a self-signed certificate or a certificate that was signed by an untrusted authority, you must use one of the `--ca-file`, `--ca-cert` or `--insecure` options or the logging agent fails to validate the server identity and does not send logs. When using `--ca-file` or `--ca-cert`, the vRealize Log Insight server certificate must be valid for the server's host name. In all cases, verify the integration by allowing a few minutes for processing and then checking that vRealize Log Insight received the logs.

`Output`

No output is expected.

`Exit codes`

The following exit codes are possible:

- 0 - The configuration was updated.
- 1 - An exception occurred as part of the execution. Examine the error message for details.

Examples - Configure or update integration configuration

```
$ vracli vrli set my-vrli.local

$ vracli vrli set 10.20.30.40

$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40

$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40

$ vracli vrli set --insecure http://my-vrli.local:8080

$ vracli vrli set --agent-id my-vrli-agent my-vrli.local

$ vracli vrli set --environment staging my-vrli.local

$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Clear integration of vRealize Log Insight

Command

```
vracli vrli unset
```

Note After you run the command, it can take up to 2 minutes for the logging agent to apply your specified configuration.

Arguments

There are no command line arguments.

Output

Confirmation is output in plain text format.

Exit codes

The following exit codes are available:

- 0 - The configuration was cleared or no configuration existed.
- 1 - An exception occurred as part of the execution. Examine the error message for details.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

How do I create or update a syslog integration in vRealize Automation

You can configure vRealize Automation to send your logging information to remote syslog servers.

The `vracli remote-syslog set` command is used to create a syslog integration or overwrite existing integrations.

vRealize Automation remote syslog integration supports the following connection types:

- Over UDP.
- Over TCP without TLS.

  Note To create a syslog integration without using TLS, add the `--disable-ssl` flag to the `vracli remote-syslog set` command.

- Over TCP with TLS.

For information on configuring logging integration with vRealize Log Insight, see How do I configure log forwarding to vRealize Log Insight.

Prerequisites

Configure one or more remote syslog servers.

Procedure

1. Log in to the vRealize Automation appliance command line as **root**.
2. To create an integration to a syslog server, run the `vracli remote-syslog set` command.

   ```
   vracli remote-syslog set -id name_of_integration protocol_type://
   syslog_URL_or_FQDN:syslog_port
   ```

   Note If you do not enter a port in the `vracli remote-syslog set` command, the port value defaults to 514.

   Note You can add a certificate to the syslog configuration. To add a certificate file, use the `--ca-file` flag. To add a certificate as plaintext, use `--ca-cert` flag.

3. (Optional) To overwrite an existing syslog integration, run the `vracli remote-syslog set` and set the `-id` flag value to the name of the integration you want to overwrite.

   Note By default, the vRealize Automation appliance requests that you confirm that you want to overwrite the syslog integration. To skip the confirmation request, add the `-f` or `--force` flag to the `vracli remote-syslog set` command.

What to do next

To review the current syslog integrations in the appliance, run the `vracli remote-syslog` command.

How do I delete a syslog integration for logging in vRealize Automation

You can delete syslog integrations from your vRealize Automation appliance by running the `vracli remote-syslog unset` command.

Prerequisites

Create one or more syslog integrations in the vRealize Automation appliance. See How do I create or update a syslog integration in vRealize Automation.

Procedure

1. Log in to the vRealize Automation appliance command line as **root**.
2. Delete syslog integrations from the vRealize Automation appliance using either of the following methods:
   - To delete a specific syslog integration, run the `vracli remote-syslog unset -id` *Integration_name* command.
   - To delete all syslog integrations on the vRealize Automation appliance, run the `vracli remote-syslog unset` command without the `-id` flag.

     Note By default, the vRealize Automation appliance requests that you confirm that you want to delete all syslog integrations. To skip the confirmation request, add the `-f` or `--force` flag to the `vracli remote-syslog unset` command.

Participating in the Customer Experience Improvement Program for vRealize Automation

6

This product participates in VMware's Customer Experience Improvement Program (CEIP). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.

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.

This chapter includes the following topics:

- How do I join or leave the Customer Experience Improvement Program for vRealize Automation
- How do I configure the data collection time for the Customer Experience Improvement Program for vRealize Automation

How do I join or leave the Customer Experience Improvement Program for vRealize Automation

Join or leave the Customer Experience Improvement Program (CEIP) from the vRealize Automation appliance command line.

You can join the CEIP program when you install vRealize Automation and with the vRealize Lifecycle Manager (LCM). You can also join or leave the program by using command line options after installation.

To join the Customer Experience Improvement Program by using command line options:

1 Log in to the vRealize Automation appliance command line as **root**.

2 Run the `vracli ceip on` command.

3 Review the Customer Experience Improvement Program information and run the `vracli ceip on --acknowledge-ceip` command.

4 To restart the vRealize Automation services, run the `/opt/scripts/deploy.sh` command.

To leave the Customer Experience Improvement Program by using command line options:

1 Log in to the vRealize Automation appliance command line as **root**.

2 Run the `vracli ceip off` command.

3 To restart the vRealize Automation services, run the `/opt/scripts/deploy.sh` command.

How do I configure the data collection time for the Customer Experience Improvement Program for vRealize Automation

You can set the day and time when the Customer Experience Improvement Program (CEIP) sends data to VMware.

Procedure

1 Log in to the vRealize Automation appliance command line as **root**.

2 Open the following file in a text editor.

`/etc/telemetry/telemetry-collector-vami.properties`

3 Edit the properties for day of week (dow) and hour of day (hod).

Property	Description
`frequency.dow=<day-of-week>`	Day when data collection occurs.
`frequency.hod=<hour-of-day>`	Local time of day when data collection occurs. Possible values are 0–23.

4 Save and close `telemetry-collector-vami.properties`.

5 Apply the settings by entering the following command.

```
vcac-config telemetry-config-update --update-info
```

Changes are applied to all nodes in your deployment.