Using VMware vRealize® Orchestrator™ with VMware vCloud® Availability for vCloud Director®

Version 1.0

April 2017

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

Contents

1. Intended Audience

This information is intended for administrators and workflow developers who want to use VMware vRealize® Orchestrator™ to automate VMware vCloud® Availability for vCloud Director® disaster recovery processes.

Some experience with vRealize Orchestrator is recommended to successfully configure vRealize Orchestrator for use with vCloud Availability for vCloud Director. vRealize Orchestrator development skills are also recommended to customize workflows. For both skill sets, a number of excellent books are available online from publishers such as Packt> and VMware Press.

1.1 Product Versions

The following products were used to test the samples in this paper.

Product	Version
vCloud Availability for vCloud Director	1.0.1
vCloud Director	8.10
vRealize Orchestrator	7.0.1
vRealize Orchestrator VMware vSphere® Replication™ plug-in	6.1.1.3850197
vCloud Director plug-in	8.10.0.3819019
vRealize Orchestrator REST plug-in	2.0.1.3415692

1.2 Document History

This is the first version of this white paper.

Version	Release Date	Authors	Reviewers
1.0	March 2017	Bob Webster	Tomas Fojta, Roger Freixa, Brandon Gordon

2. Introduction

This white paper explores the use of vRealize Orchestrator with vCloud Availability for vCloud Director.

vCloud Availability for vCloud Director is a disaster recovery solution that enables VMware vSphere users to replicate virtual machines from their on-premises data center to a Cloud managed by a VMware vCloud Air™ service provider.

vRealize Orchestrator is an automation engine that can be optionally used with vCloud Availability for vCloud Director to automate disaster recovery processes.

This paper covers a number of topics:

- Why use vCloud Orchestrator with vCloud Availability for vCloud Director
- vRealize Orchestrator deployment locations
- Installation of the vRealize Orchestrator appliance
- Initial configuration of vRealize Orchestrator for use with vCloud Availability for vCloud Director
- Sample automation workflows for disaster scenarios

3. Why Use vRealize Orchestrator with vCloud Availability for vCloud Director?

vRealize Orchestrator can be used to extend the capabilities of vCloud Availability for vCloud Director. vCloud Availability for vCloud Director is designed to manage the protection and recovery of individual virtual machines. vRealize Orchestrator can be employed as a customizable extension to vCloud Availability for vCloud Director, allowing administrators to execute complex disaster recovery workflows that coordinate multiple virtual machines.

Example workflows:

- Auto protect groups of virtual machines.
- Failover and start virtual machines in a specific order.

vRealize Orchestrator can also perform supporting tasks to customize the target DR environment. Configuration changes such as configuring load balancers, adjusting firewall settings, and changing virtual machine settings can be completed using the vRealize Orchestrator plug-in framework.

Example workflows:

- Customize virtual machine hardware settings after failover.
- Customize the failover environment. For example, making changes to Domain Name Servers and load balancers.
- Orchestrate the failover of a large group of VMs using a single REST call.

vRealize Orchestrator can also be used to automate existing or new scripts written for popular shells, such as Bash and PowerShell.

4. vRealize Orchestrator Deployment Locations

vRealize Orchestrator is based on a client-server architecture. Client applications be used to author and execute workflows that are stored on the vRealize Orchestrator server. A number of vRealize Orchestrator clients are available:

- The Java Swing client, a graphical development environment used to create and execute workflows.
- The VMware vSphere Web Client extension to vRealize Orchestrator can be configured to execute vRealize Orchestrator workflows from within the vSphere Web Client.
- Any REST capable client can be used as a vRealize Orchestrator client to invoke workflows.
- VMware vRealize Automation™ integrates with embedded or external vRealize Orchestrator and provides a service catalog, role-based access control ,and rich governance capabilities

Note vRealize Automation is not required to utilize vRealize Orchestrator with vCloud Availability for vCloud Director.

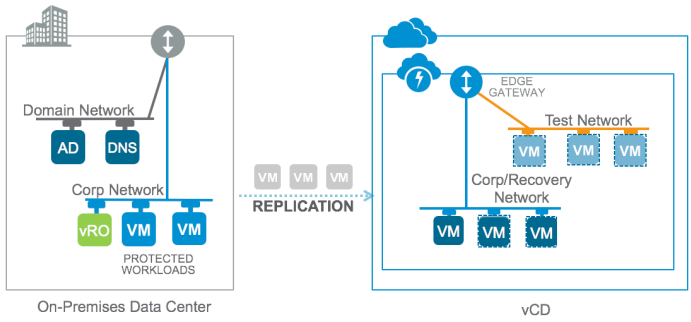
During a disaster event, the vRealize Orchestrator server must be available and accessible to tenant users to execute workflows. The following sections explore possible deployment locations for the vRealize Orchestrator server:

- Deploying vRealize Orchestrator on-premises in the tenant data center
- Deploying vRealize Orchestrator in vCloud Director
- Deploying vRealize Orchestrator both on-premises and in the cloud

4.1 On-Premises Deployment

In this deployment scenario, vRealize Orchestrator is deployed by the tenant in their on-premises data center. The tenant uses vRealize Orchestrator to configure/manage replications and test failovers.

Figure 1. On-Premises vRealize Orchestrator Server



The following is true for this scenario:

- Primary use is replication configuration and failover tests executed from the on-premises data center.
- A vRealize Orchestrator cloud deployment is additionally required to perform automation in the cloud during on-premises site failure.

4.2 In-the-Cloud Deployment

In this scenario, vRealize Orchestrator is deployed in a virtual data center in the Cloud.

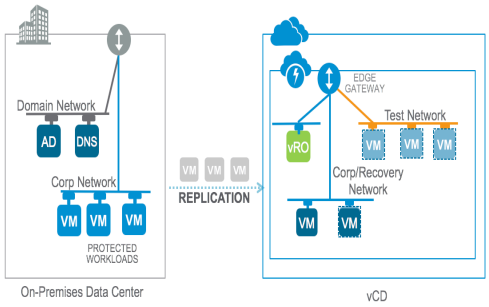


Figure 2. Tenant Deployed vRealize Orchestrator in-the-Cloud

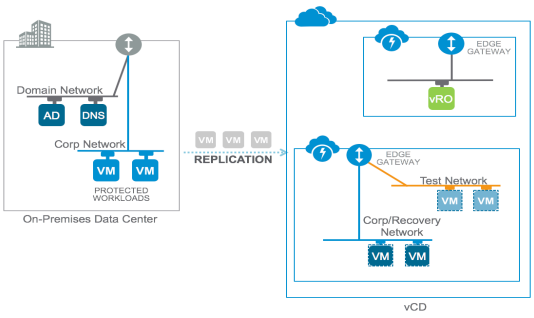


Figure 3. vRealize Orchestrator Deployed by Cloud Provider

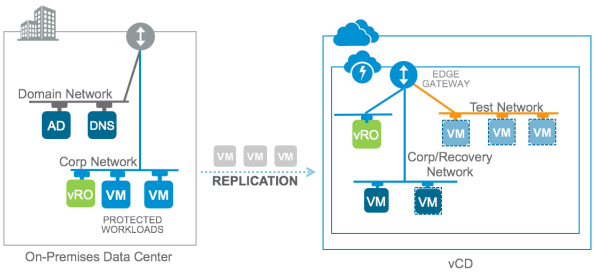
The following is true for this scenario:

- vRealize Orchestrator can be deployed and managed by the cloud provider or deployed by the tenant in to their own virtual data center.
- Optionally, vRealize Orchestrator can be configured to have access to the on-premises data center using a VPN or direct connect network.

4.3 On-Premises and In-the-Cloud Deployment

This scenario is a combination of the earlier deployment options. A vRealize Orchestrator appliance is deployed both on-premises and in the Cloud. The cloud deployment can be managed by the tenant or the cloud provider.

Figure 4. Dual vRealize Orchestrator Deployment



The following is true for this scenario:

- On-premises vRealize Orchestrator appliance manages all automation tasks during normal operations of the on-premises data center.
- Cloud vRealize Orchestrator manages cloud automation tasks when the on-premises vRealize Orchestrator is unavailable.
- Workflows for cloud recovery are exported from the on-premises vRealize Orchestrator and imported into the cloud vRealize Orchestrator.

5. Install vRealize Orchestrator and Java Client

This section describes the steps to deploy the vRealize Orchestrator appliance on either VMware vCenter® or vCloud Director.

The installation steps in the vRealize Orchestrator documentation describe how to deploy the vCloud Director appliance on vCenter.

In summary, the steps are as follows:

1. Deploy the appliance to an existing virtual data center as an OVF deployment. During deployment, set the required appliance properties. Power on the appliance.
2. Test the appliance configuration. Log in to the vRealize Orchestrator Control Center and configure an authentication provider.
3. Install the vSphere Replication plug-in.
4. Download the vRealize Orchestrator client using the **Download Orchestrator Client Installable** link on the Control Center.
5. Start the client and verify the user can log in to the server using the vRealize Orchestrator client.

5.1 Deploy the Appliance to an Existing Virtual Data Center

Note Installing vRealize Orchestrator directly on vCloud Director requires slight changes to the installation process. See Section 5.1.2, For vCloud Director.

5.1.1 For vCenter

Perform the following steps to deploy the appliance.

1. Download the vRealize Orchestrator appliance from my.vmware.com
2. Deploy the appliance as an OVF using the vSphere Web Client.
   a. Accept EULA.
   b. Pick a target folder for the deployment.
   c. Select provisioning type and datastore.
   d. Select target network.
   e. Set the appliance password for root user.
   f. Select the **Enable SSH** check box.
   g. Enter the required guest properties to complete the appliance deployment. If using DHCP, accept the network defaults or enter network values for static network definition.
   h. Power on the appliance.
   i. Go to Section 5.2, Test the Appliance Configuration.

5.1.2 For vCloud Director

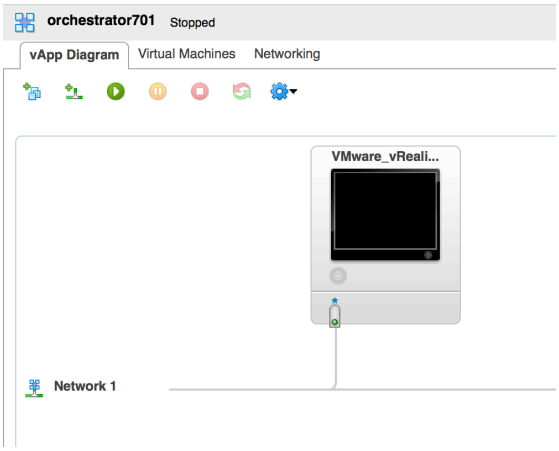
When deploying vRealize Orchestrator to vCloud Director, the appliance properties supplied to the OVF deployment wizard are ignored.

The following steps detail how to manually set the properties and configure vApp networking.

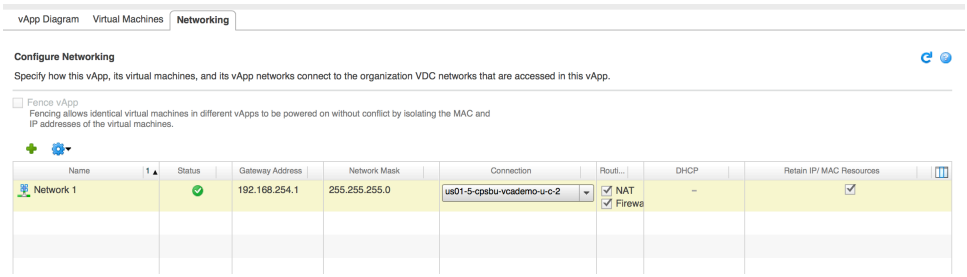
1. Deploy the appliance to an existing virtual data center as an OVF deployment using the vCloud Director console or ovftool. The following is a sample OVF deployment:

   ```
   ovftool --acceptAllEulas "/Volumes/Orchestrator/VMware-vRO-Appliance-
   7.0.1.17606-3571217_OVF10.ovf"
   "vcloud://bwebster_local:@vcore.vmware.com/cloud/org/us01-5-cpsbu-vcademo-
   u/?org=us01-5-cpsbu-vcademo-u&vdc=us01-5-cpsbu-vcademo-
   ovdc1&vapp=orchestrator701"
   ```

2. After the deployment completes, enter the vCloud Director console and open the vApp diagram. The vApp should contain **Network 1** as shown in the following screen shot.



3. Click the Networking tab and select an external network connection for Network 1. Select the **NAT**, **Firewall**, and **Retain IP / MAC Resources** check boxes.

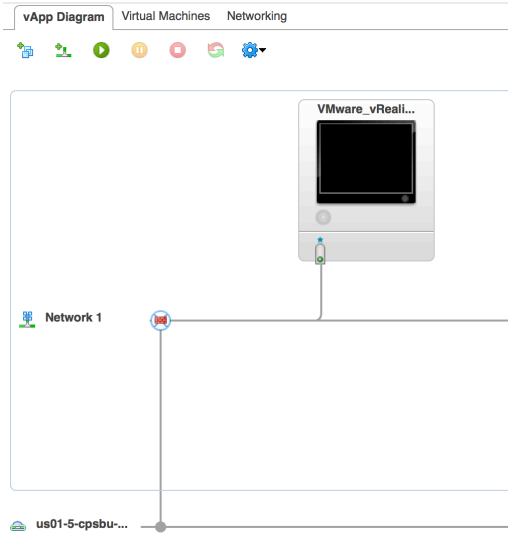


   Click **Apply**.

4. Return to the vApp Diagram tab.

   Network 1 should now have gateway symbol containing a firewall icon as shown in the following figure.

   Figure 5. vApp Containing vRealize Orchestrator



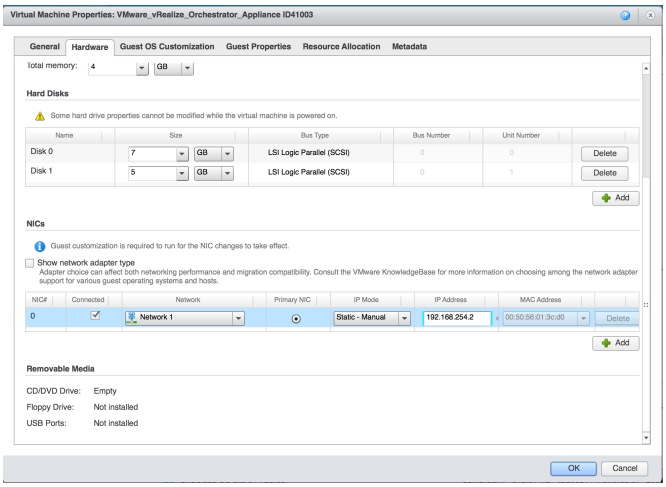
5. Right-click the VM in the vApp Diagram and choose the **Properties** menu item.

   a. Select the Hardware tab.

   b. In the NICs section, change the IP mode to **Static – Manual**.

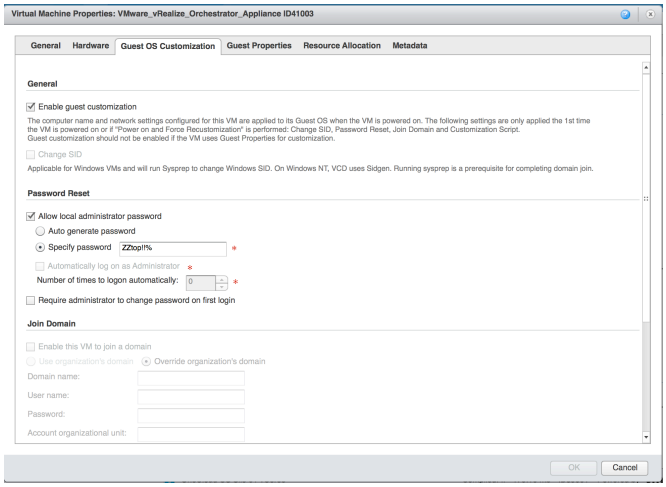
   c. Set the IP address to 192.168.254.2.

   Note This step is required because NAT rules cannot be configured for DHCP addresses.



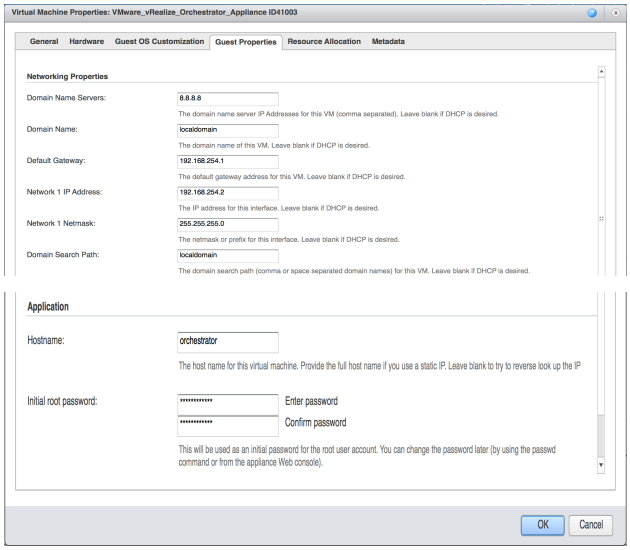
d. Select the Guest OS Customization tab. Note the value of the generated root login appliance password.

Figure 6. Virtual Machine Properties



e. Select the Guest Properties tab. Enter the required networking properties. Leave the existing setting for initial root password. Click **OK** to save the settings.

Figure 7. Guest Properties



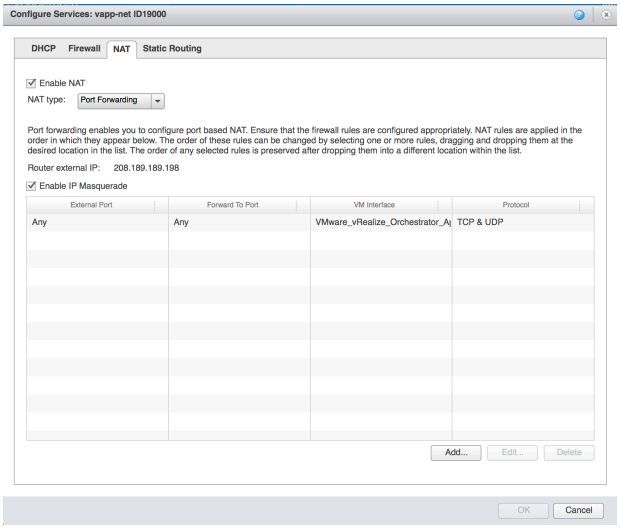
6. Power on the vApp.

7. Set default NAT rules:

   a. Right-click **Network 1** in the vApp Diagram and choose **Configure Services**. Select the NAT tab.

   b. Create a port-forwarding NAT rule for TCP and UDP as shown in the following figure.

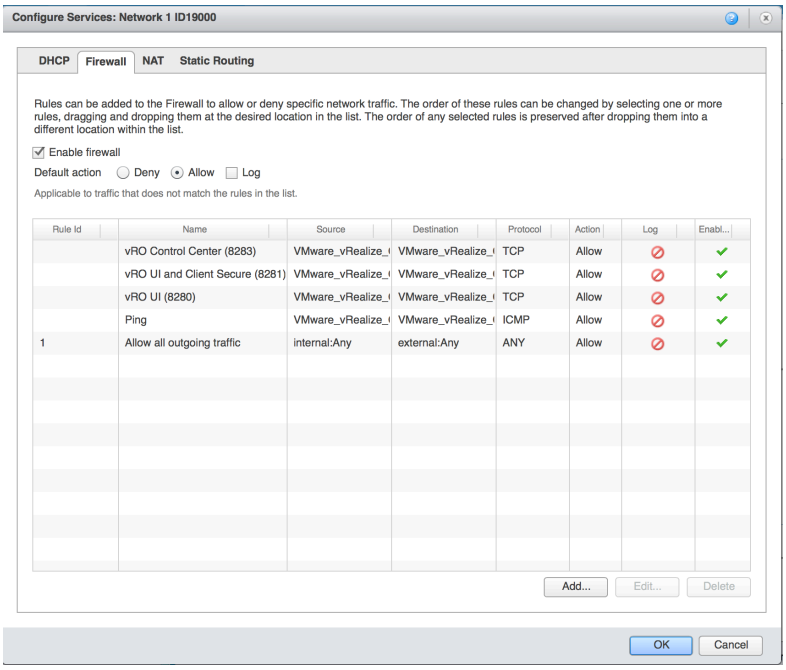
Figure 8. NAT Rules



8. Configure firewall rules:

   Select the Firewall tab. Enter firewall rules that match the rules shown in the following figure. When creating rules, use **NAT IP** for the source and **Assigned IP** for the target. Click **OK** to save the rule settings.

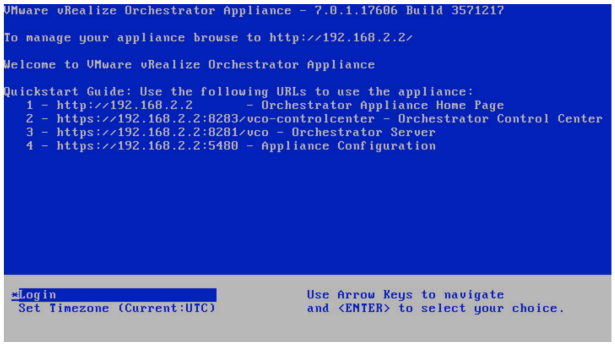
Figure 9. Firewall Rules



5.2 Test the Appliance Configuration

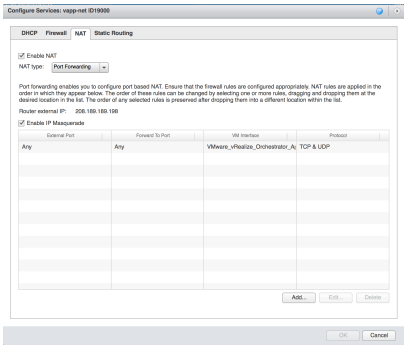
1. Power on the appliance and check the console to confirm the appliance has an IP address on the network.

Figure 10. vRealize Orchestrator Appliance Console



Note With vCloud Director, when using NAT to access the vRealize Orchestrator, the IP address used externally will be the gateway IP address rather than the IP address listed on the appliance home page. This NAT service IP can be retrieved from the vApp Networking tab.

Figure 11. NAT GW Address

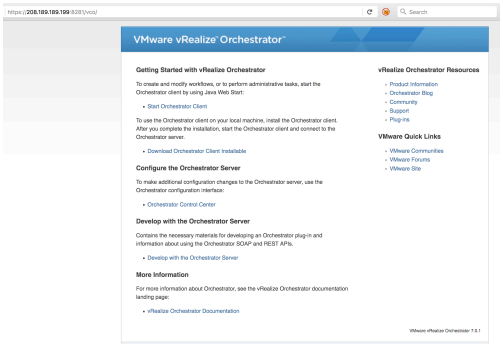


So in the example above, the vRealize Orchestrator appliance home page URL is:

https://208.189.189.199:8281/vco/

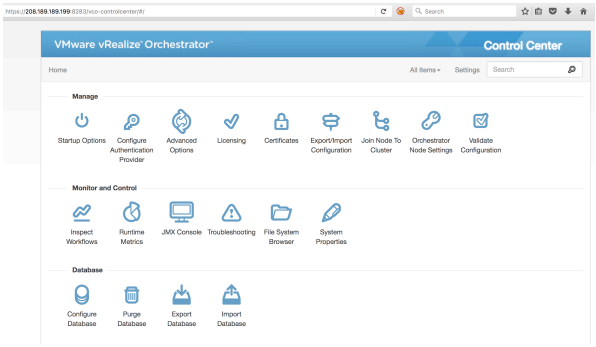
2. Use a browser to confirm access to the vRealize Orchestrator appliance home page.

Figure 12. vRealize Orchestrator Appliance Home Page



3. Click the **Orchestrator Control Center** link to confirm access to the Control Center. When challenged by the browser, log in using the appliance username **root** and the auto generated password, which is visible in the VM settings – Guest OS Customization tab.

Figure 13. vRealize Orchestrator Control Center

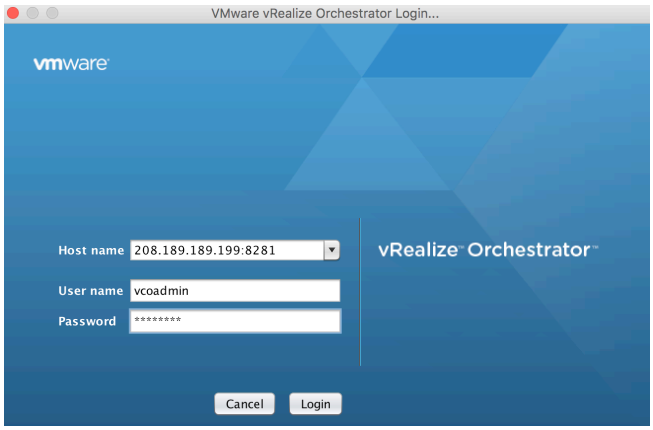


4. Test the vRealize Orchestrator client login.

   a. Return to the appliance home page and click the **Start Orchestrator Client** link. The vRealize Orchestrator Java Web Start client should load.

   b. Log in using the credentials **vcoadmin** / **vcoadmin**. This tests the Java client using the default LDAP authenticator.

Figure 14. vRealize Orchestrator Java Client



5.3 Install the vSphere Replication 6.1.1 Plug-In

1. Download the plug-in from my.vmware.com.

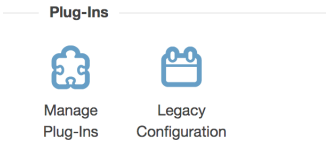
   https://my.vmware.com/group/vmware/details?downloadGroup=VR_VRO_PLUGIN_611&productId=491

   The download produces a 12 MB file named `vr-6.1.1.vmoapp`.

2. Log in to the vRealize Orchestrator Control Center using the appliance **root** / *generated-appliance-credential*.

3. Click **Manage Plug-Ins**.

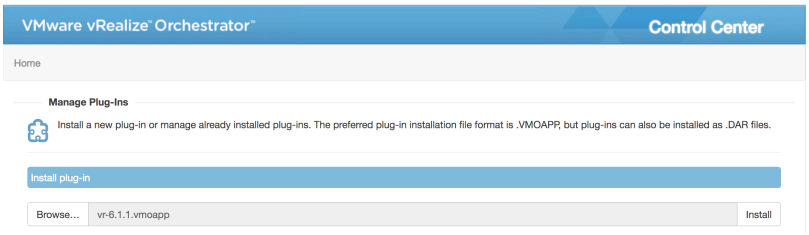
   Figure 15. Control Center Plug-Ins



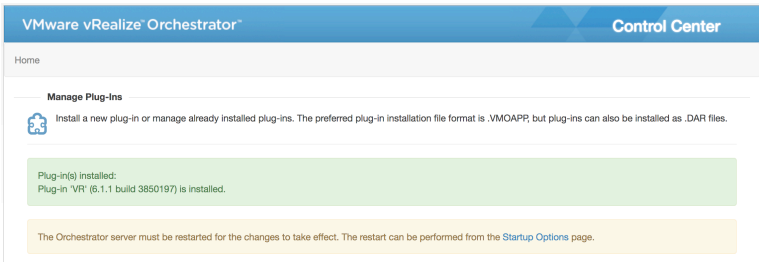
4. Browse and select the downloaded the plug-in file – `vr-6.1.1.vmoapp`.

5. Select the **Accept EULA** check box. Click **Install**.

   Figure 16. Adding an Orchestrator Plug-In



   A success message should be displayed.



6. Click the **Startup Options** link in the message to go to the Startup Options page.

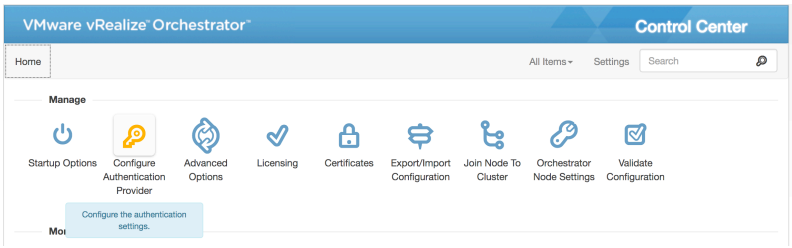
7. On the Startup Options page, click **Restart** .

5.4 Configure a vCenter Authenticator

This step reconfigures vRealize Orchestrator to use vCenter for authentication instead of the default embedded LDAP Server. The **vcoadmin/vcoadmin** credentials will no longer work once vCenter authentication is configured.

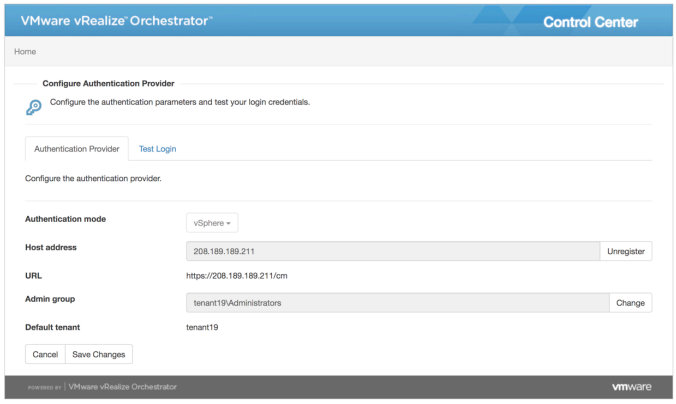
1. Click the **Configure Authentication Provider** link.

Figure 17. Configure Authentication Provider



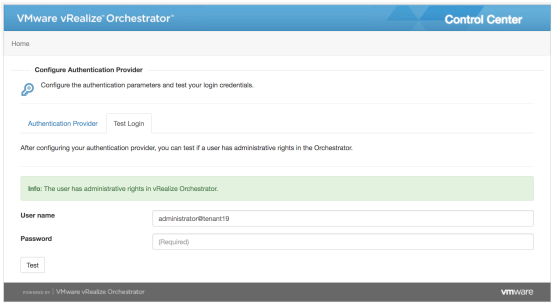
2. Enter the vCenter IP address or host name. Then browse for and select an Administrator's group that is prefixed by the vCenter domain name. Set the Default Tenant value to the same domain name.

Figure 18. vSphere Authenticator Provider Settings



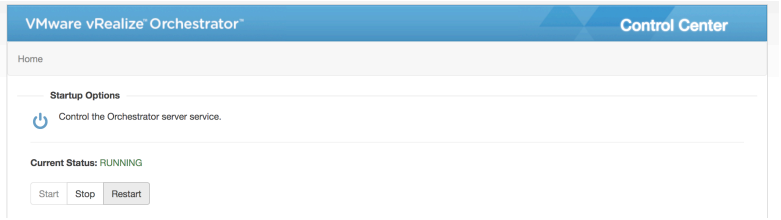
3. Test the authenticator. Select the Test Login tab and confirm the login is successful.

Figure 19. Authenticator Credentials



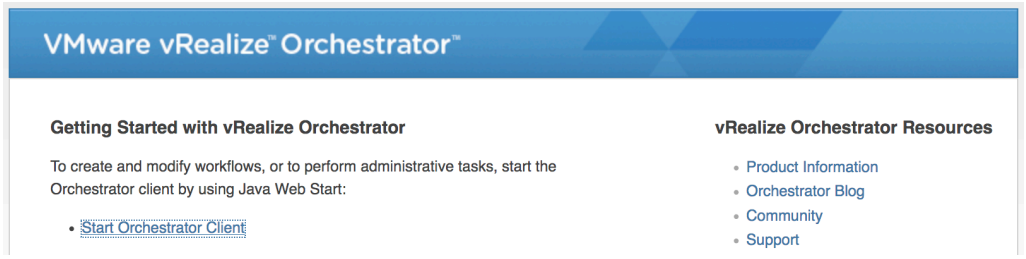
4. Restart the service.

Figure 20. Restart vRealize Orchestrator



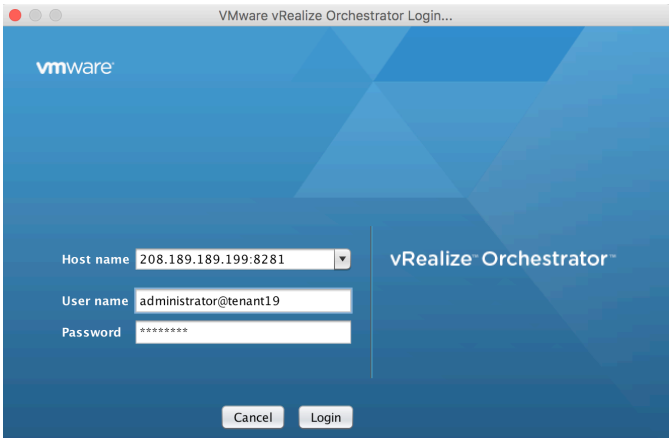
5. Start the Java client.

Figure 21. vRealize Orchestrator Client Link



6. Test the login using vCenter credentials.

Figure 22. vRealize Orchestrator



Note It the Java client login fails with the error Java Client Error : Current Node is not active, enable the Java console in the client browser and examine the stack trace. If the error is **could not connect over REST to server xxx.xxx.xxx.xxx on port 8281 org.springframework.web.client.HttpServerErrorException: 503 STANDBY**, the most likely cause is the wrong Default Tenant name was supplied to the authenticator configuration. For example, vsphere.local instead of tenant19 for administrator@tenant19.

6. Configuring Orchestrator for Use with vCloud Availability for vCloud Director

This section provides detailed instructions to configure an existing vRealize Orchestrator server for use with vCloud Availability for vCloud Director.

To utilize vRealize Orchestrator with vCloud Availability for vCloud Director, a one-time configuration setup is necessary.

The high level steps are:

1. Install the vSphere Replication plug-in.
2. (Optional).Install the vCloud Director plug-in
3. (Optional) Configure the HTTP-REST plug-in.
4. Configure inventory items in vRealize Orchestrator:
    a. Register tenant VMware vCenter Server® nodes.
    b. Register cloud site credentials.
    c. Register standalone organizations.
    d. (Optional) Register vCloud Director endpoint.

6.1 Installing the vSphere Replication Plug-In

The vSphere Replication plug-in provides workflows that automate the configuration, testing, and failover of protected workloads. The plug-in leverages the vSphere Replication API to access replication operations.

To install the vSphere Replication plug-in, complete the following steps:

1. Download the vSphere Replication vRealize Orchestrator plug-in from the my.vmware.com download site.
2. Install the plug-in using the vRealize Orchestrator Control Center user interface. These steps are detailed in Section 5.3, Install the vSphere Replication 6.1.1 Plug-In.

6.2 Installing the vCloud Director Plug-In

The vCloud Director plug-in provides workflows that automate vCloud Director organizations and virtual data centers. The plug-in leverages the vCloud Director API to provide capabilities. This plug-in is only required to perform automations against the recovered virtual machines protected on the cloud provider site. For example, to change the memory settings or IP address of a virtual machine after failover.

To install the vCloud Director plug-in, complete the following steps:

1. Download the vCloud Director vRealize Orchestrator plug-in from the my.vmware.com download site.
2. Install the plug-in using the vRealize Orchestrator Control Center user interface.

6.3 Configuring the HTTP-REST Plug-In

The HTTP-REST plug-in is included with vRealize Orchestrator. No installation is required. The plug-in can be configured to provide access to the complete vCloud Availability for vCloud Director API exposed by vCloud Director. For complete configuration instructions see Appendix B: Accessing vCloud Availability for vCloud Director Using the HTTP-REST Plug-In.

6.4 Configuring Inventory Items in Orchestrator

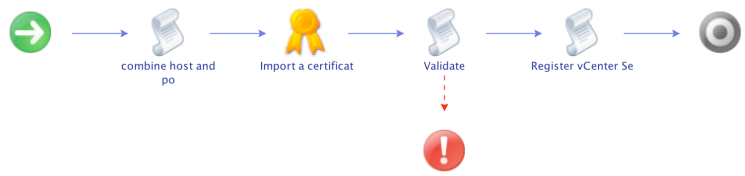
To execute workflows, input parameters of different types are supplied. When an input parameter represents an existing vCenter or vCloud Director instance, a reference to the endpoint must exist in the vRealize Orchestrator Inventory.

Part of the initial configuration required when using vRealize Orchestrator with vCloud Availability for vCloud Director, is running workflows to register the on-premises vCenter and Cloud vCloud Director Organizations that will be inputs to disaster recovery workflows.

6.4.1 Registering Tenant vCenter Server Nodes

The **Add a vCenter Server Instance** workflow is used to register a vCenter Server in the vRealize Orchestrator inventory. This is typically a tenant on-premises vCenter instance. The script is located in the vCenter workflow folder that is part of the base vRealize Orchestrator product.

Figure 23. Add a vCenter Server Instance Workflow

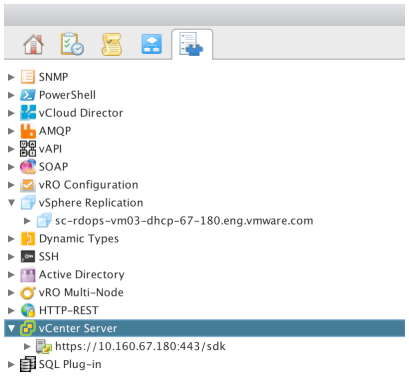


The same workflow also automatically discovers vSphere Replication appliances registered with the vCenter Server and adds them to the vSphere inventory. Run the **Add a vCenter** workflow once for each vCenter Server on the tenant site that will host replicated virtual machines.

Caution Do not run this workflow before the vSphere Replication plug-in is added to the vRealize Orchestrator, because the vSphere Replication appliances will not be discovered and added to the inventory.

After the workflow has been executed, a vCenter Server node should be visible in the vRealize Orchestrator inventory. The vSphere Replication server associated with the vCenter Server node should also be visible.

Figure 24. vCenter and vSphere Replication Servers in vRealize Orchestrator Inventory



See Section 8, Example Workflows for a detailed example of how to run this workflow.

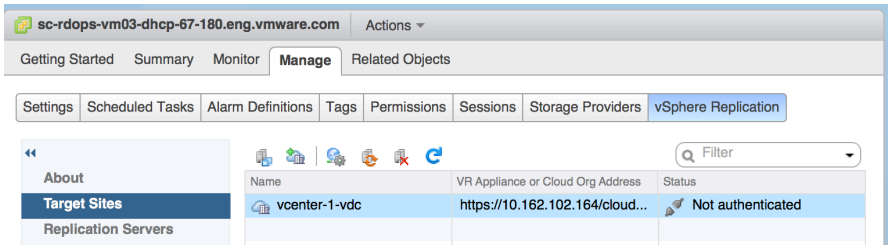
6.4.2 Registering Cloud Site Credentials

The **Register Cloud Site** workflow stores credentials required to authenticate against a defined vCloud Director Cloud target defined in the vRealize Orchestrator database.

Figure 25. Register Cloud Site Workflow Schema

The credentials are needed by workflows such as **Configure Replication** that interact with the tenant vSphere Replication appliance. At the time the workflow runs, the authentication connection from the vSphere Replication server to the remote site might have expired as shown in the following screen shot.

Figure 26. Disconnected Target Site



Running the **Register Cloud Site** workflow stores the credentials needed by vRealize Orchestrator for vCloud Director to authenticate the remote connection. Run the **Register Cloud Site** workflow once for each vCloud Director target site defined in the tenant vSphere Replication appliance.

6.4.3 Registering Standalone Organizations

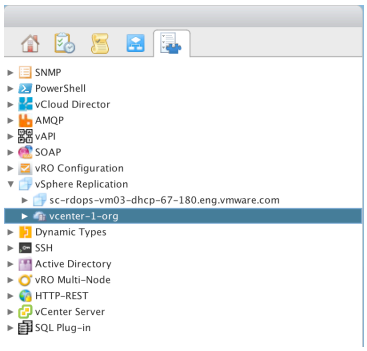
The **Register a Standalone Organization** workflow is used to register an endpoint and credentials for an organization and virtual data center in a vCloud Director instance.

Figure 27. Register Standalone Organization Workflow Schema

Workflows that run directly against the Cloud site such as **Run Test Recovery at Cloud Site** require the cloud endpoint to be added to the vRealize Orchestrator inventory in advance.

Run the **Register a Standalone Organization** workflow once for each virtual data center running on the provider that will host replicated virtual machines.

Figure 28. Standalone Organization in vRealize Orchestrator Inventory



See Section 8, Example Workflows for a detailed example of how to run this workflow.

6.4.4 Registering a vCloud Director Endpoint

The **Add a Connection** workflow is used to register a vCloud Director endpoint and credentials.

This step is optional. This endpoint is utilized by the vCloud Director Orchestrator plug-in. It is only necessary to support workflows that automate virtual machines running on vCloud Director.

Figure 29. Add a vCloud Director Connection Workflow Schema

Workflows that run against virtual machines running on a Cloud site such as **Change Memory Capacity of a Virtual Machine**, require the vCloud Director endpoint to be added to the vRealize Orchestrator inventory in advance. This workflow adds the vCloud Director server endpoint to the vRealize Orchestrator inventory and supports workflows that automate an entire organization within vCloud Director. This is different than the **Register Standalone Organization** workflow discussed earlier, which registers an organization with the vSphere Replication plug-in and allows only replication-related operations to be performed on a Cloud endpoint.

Run the **Add a Connection** workflow once for each vCloud Director instance/service provider. After the workflow executes, the server should be visible in the vRealize Orchestrator inventory as shown in the following screen shots.

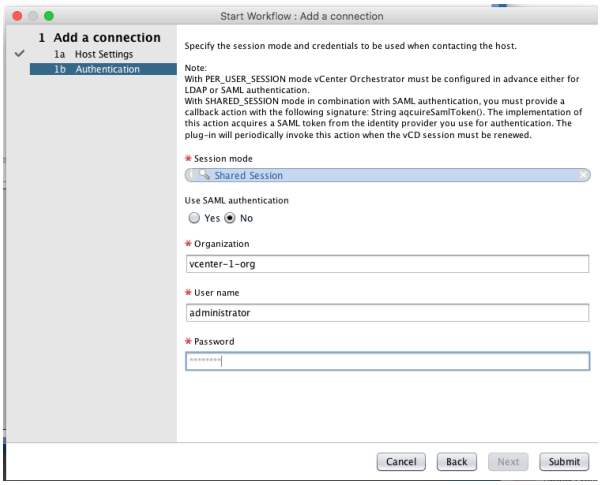


Figure 30. Add a Connection Authentication Settings

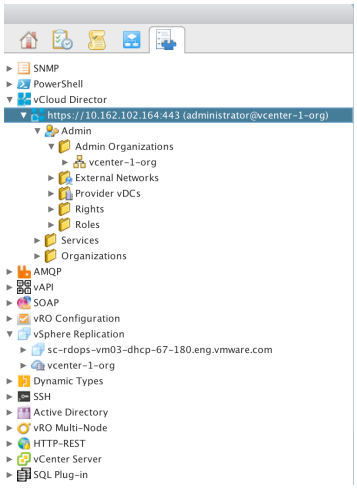
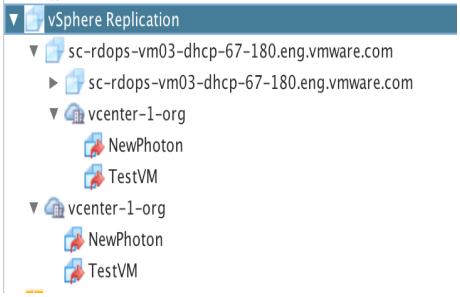


Figure 31. vCloud Director Server Connection Shown in vRealize Orchestrator Inventory

6.4.5 vRealize Orchestrator Inventory

When the configuration steps are completed, new inventory nodes should appear in the vRealize Orchestrator inventory similar to the ones shown in the following figure.

Figure 32. vRealize Orchestrator Inventory Types

Orchestrator Inventory Tree	Object Type	Comment
	Site [1]	vSphere Replication Server on Tenant
	VcRemoteSite	vCenter Replication Target
	CloudVdcRemoteSite	vCloud Director Replication Target
	VcToCloudSourceGroup	Source side of replication
	VcToCloudSourceGroup	Source side of replication
	StandaloneOrg [2]	vSphere Replication Server on Provider
	VcToCloudTargetGroup	Target side of replication
	VcToCloudTargetGroup	Target side of replication

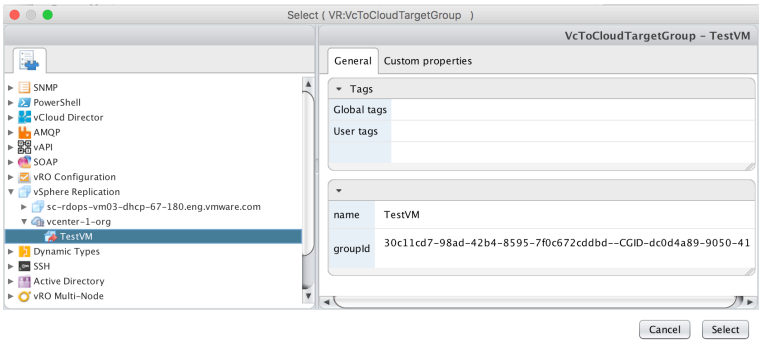
[1] Added to inventory by **Add a vCenter Server Instance** workflow.

[2] Added to inventory by **Register Standalone Organization** workflow.

Objects in the vRealize Orchestrator inventory are supplied to workflows as input parameters. The vRealize Orchestrator object browser will validate the input object type to confirm it matches the type of the required parameter. Only when a type matches the required type, will the **Select** button be enabled.

For example, as shown in the following screen shot, a parameter of type **VcToCloudTargetGroup** is required (as indicated by the value in the upper-right corner of the object browser). If an object of the wrong type is selected, the **Select** button will not be enabled.

Figure 33. Selecting the Correct Parameter Type

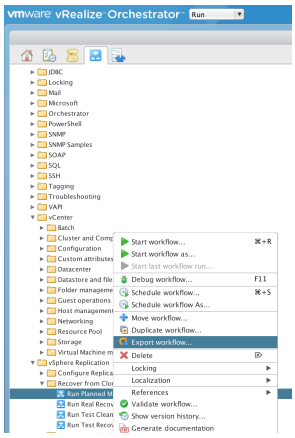


6.5 Exporting and Importing Workflows

Workflow developers can author workflows in one vRealize Orchestrator instance and copy the workflows to another vRealize Orchestrator instance using the Export/Import function of the vRealize Orchestrator client.

In deployments where vRealize Orchestrator is running on both the tenant on-premises data center and the Cloud, this enables developers to create workflows in one server and copy them to another. When relocating scripts, care must be taken to ensure that workflows will have access to the required tenant or cloud resources at the time of execution.

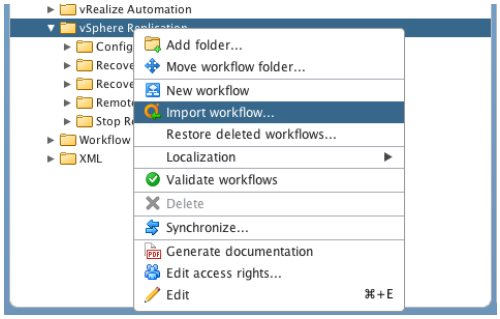
Figure 34. Exporting a Workflow Using the Orchestrator Java Client



An exported workflow is saved to a file with a `.workflow` extension on the local file system of the workstation browser.

The same file can be imported into another vRealize Orchestrator instance as shown in the following figure.

Figure 35. Importing a Workflow using the vRealize Orchestrator Java Client

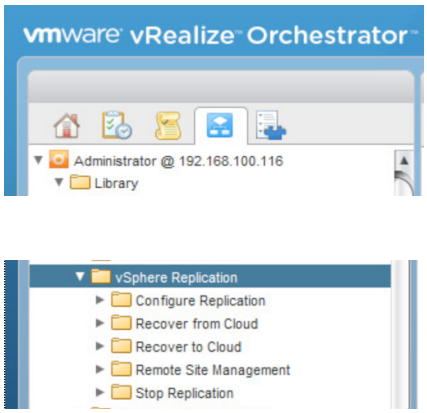


Individual workflows or complete vRealize Orchestrator packages can be exported. A package makes sure that workflows and all dependencies of the workflow are also exported. See the vRealize Orchestrator documentation for more detail.

7. Authoring Workflows for Disaster Scenarios

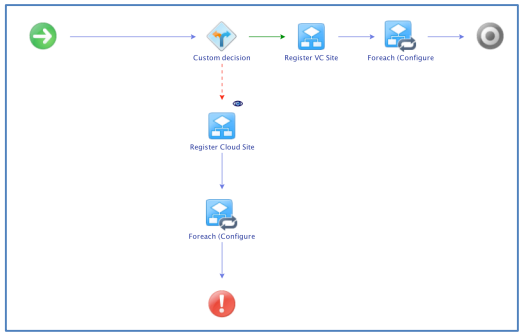
The vSphere Replication plug-in for vRealize Orchestrator provides a number of workflows that can be utilized with vCloud Availability for vCloud Director. When the plug-in is installed, the workflows are added to the set of vRealize Orchestrator workflows under the workflows tab as shown in the following screen shot.

Figure 36. Workflow Included with the vSphere Replication Plug-in



Workflow developers can use the sample workflows individually or combine them to create custom workflows. The vRealize Orchestrator Java client provides the ability to modify the supplied workflows or combine them into new custom workflows as shown in the following figure.

Figure 37. Sample Included Workflow : Protect Multiple VMs Workflow



A complete list of the workflows included with the vSphere Replication plug-in is provided in Appendix A: vSphere Replication Workflows.

Note The vRealize Orchestrator plug-in for vSphere Replication 6.0 does not provide on-premises-to-cloud pairing workflows. You must use the vSphere Web Client to pair the source on-premises vSphere Replication server with the target vCloud Director cloud site prior to executing workflows that require a replication pair.

7.1 Workflow Targets

The vSphere Replication workflows can be divided into two categories based on the inventory endpoints they require. Some workflows require a connection to the replication appliance in the on-premises data center while other workflows require only a connection to vCloud Director in the Cloud.

For example, consider the following two included workflows:

- Run Test Recovery to Cloud

  Executes a test recovery of a VM at a cloud provider data center. The workflow connects to the on-premises data center to retrieve the VM / Cloud Endpoint Pair information.

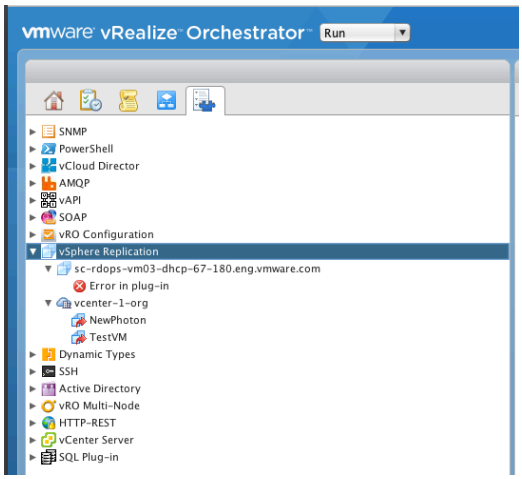
- Run Test Recovery at the Cloud Site

  Executes a test recovery of a VM at a cloud provider data center. The workflow connects to the Cloud site and does not require a connection to the on-premises site.

Workflows that connect to the on-premises vSphere Replication appliance use the configuration to determine the cloud endpoint. These workflows depend on the availability of the replication appliance in the tenant data center, and therefore should not be used for disaster workflows where the on-premises site will not be available during the outage.

For example, in the inventory shown in the following screen shot, the vSphere Replication plug-in in vRealize Orchestrator has two registered connections—one with the vSphere Replication server in the tenant data center named **sc-rdops-vm03-dhcp-67-180.eng.vmware.com** and another connection to a virtual data center named **vcenter-1-org** at a cloud provider. The vSphere Replication appliance at the tenant data center has a **Error in plugin-in** message, indicating that the appliance is not available (due in this case to a tenant outage). However, the **vcenter-1-org** node in the inventory represents the virtual data center at the cloud provider, and the endpoint is available for DR operations.

Figure 38. Disconnected Plug-In Connection



8. Example Workflows

This section provides detailed examples of several workflows that implement DR use cases:

- Add a Tenant vCenter instance to the vRealize Orchestrator inventory. (Provided by vSphere Replication plug-in.)
- Add a provider cloud site to the vRealize Orchestrator inventory. (Provided by vSphere Replication plug-in.)
- Configure replication to the Cloud. (Provided by vSphere Replication plug-in.)
- Run test recovery to the Cloud. (Provided by vSphere Replication plug-in.)
- Protect virtual machines in a folder (custom example).

8.1 Add a Tenant vCenter Instance to the vRealize Orchestrator Inventory

vRealize Orchestrator includes a built-in workflow to register vCenter Server nodes. The **Add a vCenter Server Instance** workflow is executed once to add an existing vCenter Server instance in the tenant data center to the vRealize Orchestrator inventory.

When the vRealize Orchestrator plug-in for vSphere Replication is also installed, the plug-in automatically discovers the vSphere Replication instances on all vCenter Server nodes that are currently registered.

8.1.1 Prerequisites

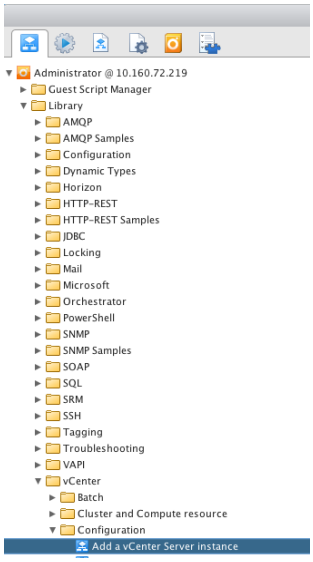
The following are prerequisites to adding a Tenant vCenter instance to the vRealize Orchestrator inventory:

- The vSphere Replication add-on has been installed in the vRealize Orchestrator instance.
- Do not run this workflow before the vSphere Replication plug-in is added to the vRealize Orchestrator because the replication appliances will not be discovered.

The following object must exist in the vRealize Orchestrator inventory:

- Workflow input—a vCenter Server endpoint URL and credentials

Figure 39. Add a vCenter Server Instance Workflow



8.1.2 Workflow Execution Steps

1. Right-click the object and choose **Start Workflow** from the context menu.
2. Enter the IP address and port for the vCenter Server. Then enter the connection credentials.

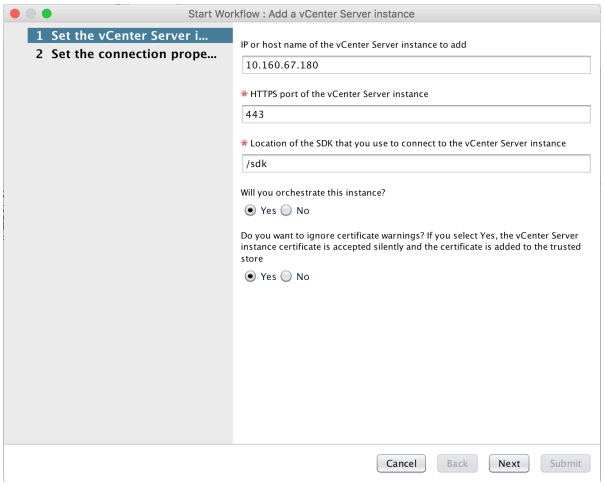


Figure 40. vCenter Server Connection Information

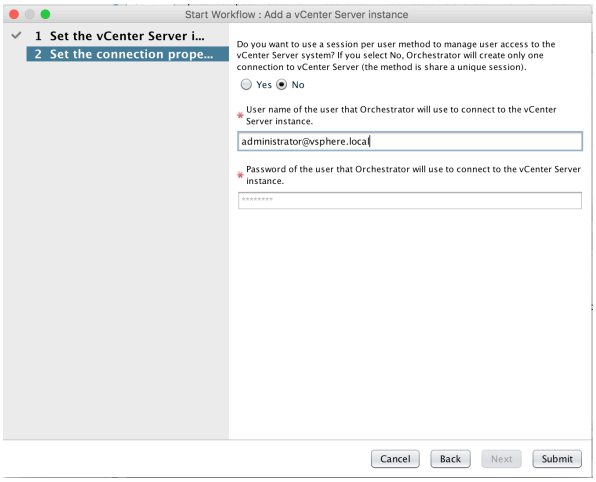


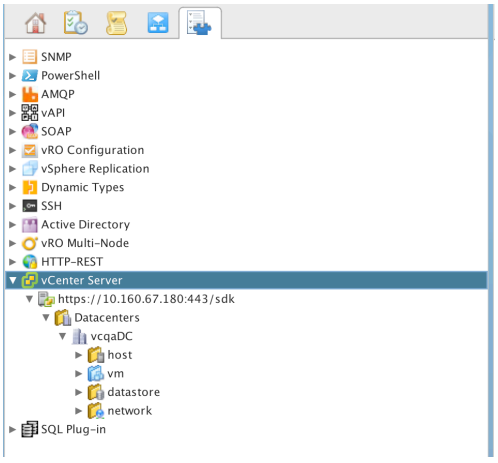
Figure 41. vCenter Server Credentials

Note Select **No** for the session sharing option to avoid an **Invalid Credentials** error on the new vCenter Server node in the vRealize Orchestrator inventory.

3. Click **Submit** to execute the workflow.

When the workflow completes, the inventory is updated to include the new vCenter instance as shown in the following figure.

Figure 42. vCenter Server in vRealize Orchestrator Inventory



8.2 Add a Provider Cloud Site (Standalone Org) to the vRealize Orchestrator Inventory

The vSphere Replication plug-in includes a workflow named **Register Standalone Organization** that adds an existing vCloud Director virtual data center to the vRealize Orchestrator inventory.

Note The workflow is not used to register a remote vCloud Director virtual data center with the tenant vSphere Replication server. Cloud targets defined on the tenant on-premises site must be defined using the vSphere Web Client.

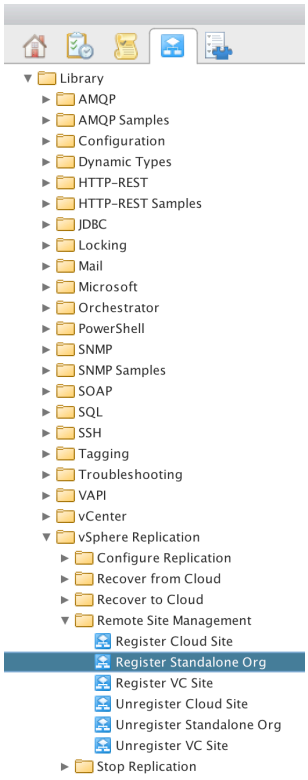
8.2.1 Prerequisites

The vSphere Replication add-on has been installed in the vRealize Orchestrator.

The following object must exist in the vRealize Orchestrator inventory:

- Workflow input—A vCloud Director URL, organization, and credentials.

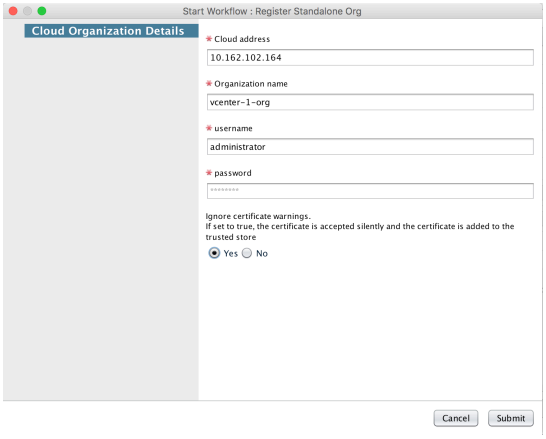
Figure 43. Register Standalone Organization Workflow



8.2.2 Workflow Execution Steps

1. Right-click the object and choose **Start Workflow** from the context menu.
2. Enter the vCloud Director IP address.
3. Enter the Organization name.
4. Enter the Organization user credentials.

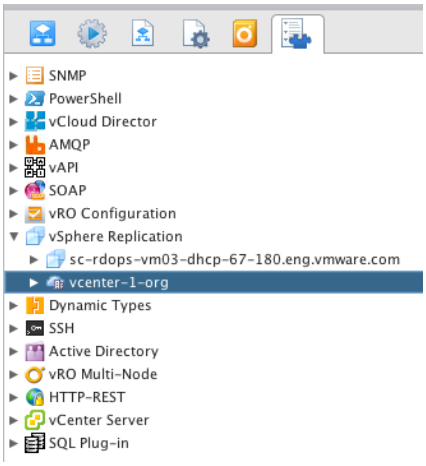
Figure 44. Cloud Organization Details



5. Click **Submit** to execute the workflow.

When the workflow completes, the inventory is updated to include the new virtual data center as shown in the following figure.

Figure 45. vCloud Director Standalone Organization in vRealize Orchestrator Inventory



There are now two different vSphere Replication servers in the inventory—the vSphere Replication server running on the tenant vCenter Server and the one associated with the replication-enabled virtual data center in the Cloud.

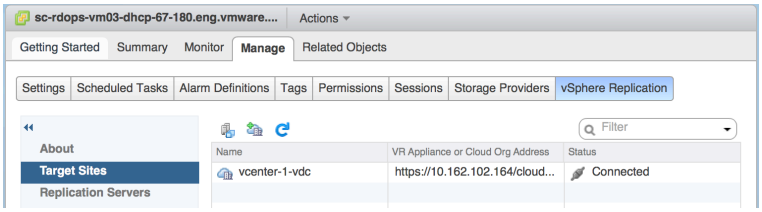
8.3 Configure Replication to the Cloud

8.3.1 Prerequisites

This workflow runs against a vSphere Replication server defined in the vRealize Orchestrator inventory.

A cloud provider target VDC must already be configured in the tenant vSphere Replication server. This must be done using the vSphere Web Client. The following figure shows a target site named **vcenter-1-vdc**.

Figure 46. A Cloud Target Site



The **Register Cloud Site** workflow should have been executed to store the login credentials for the remote site in the vRealize Orchestrator database. The **Configure Replication to Cloud** workflow will attempt to use the existing connection from the tenant vSphere Replication appliance to the remote cloud site. At the time the workflow runs, if the authenticated connection from the vSphere Replication server to the remote site has expired, vRealize Orchestrator will use the credentials stored by the **Register Cloud Site** workflow to re-establish the remote connection.

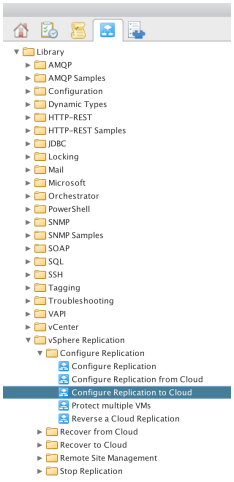
The following objects must exist in the vRealize Orchestrator inventory:

- Workflow input—A tenant vSphere Replication server
- Workflow input—A vCloud Director cloud target defined on the replication server

8.3.2 Workflow Execution Steps

1. Select the **Configure Replication to Cloud** workflow from the Workflow tab in the vRealize Orchestrator client.

   Figure 47. Configure Replication to Cloud Workflow



2. Right-click the object and select **Start Workflow** from the context menu.

3. Select the replication appliance on vCenter.

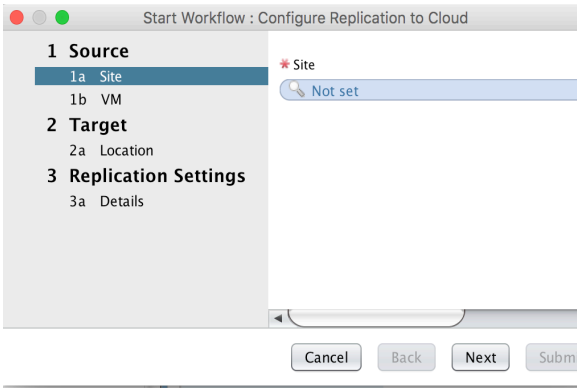


Figure 48. Browse for Source Site

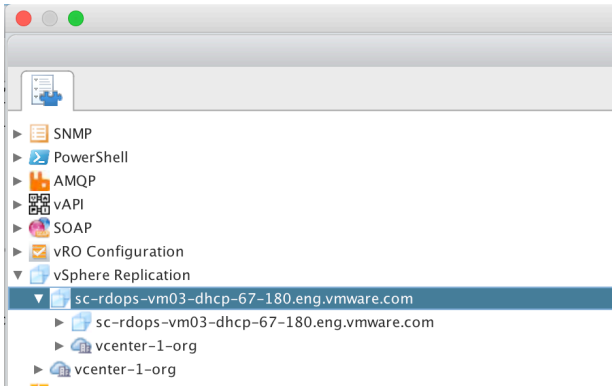


Figure 49. Select vSphere Replication Server

4. Select the virtual machine to replicate.

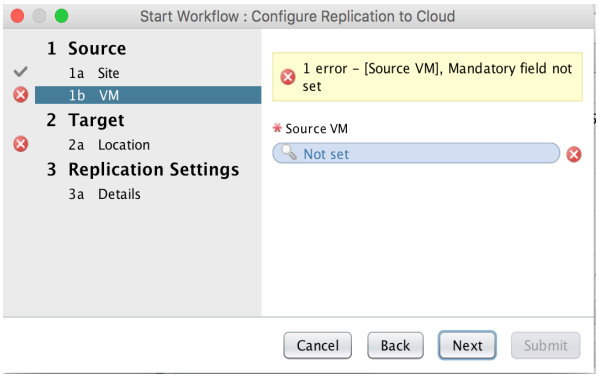


Figure 50. Browse for Virtual Machine

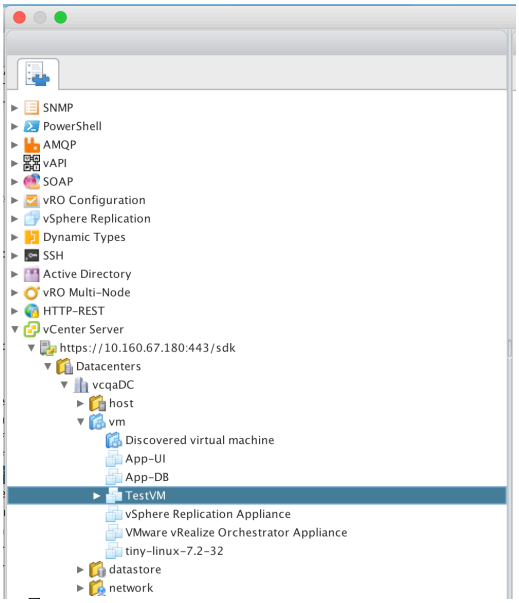


Figure 51. Select Virtual Machine

5. Select the Cloud target site.

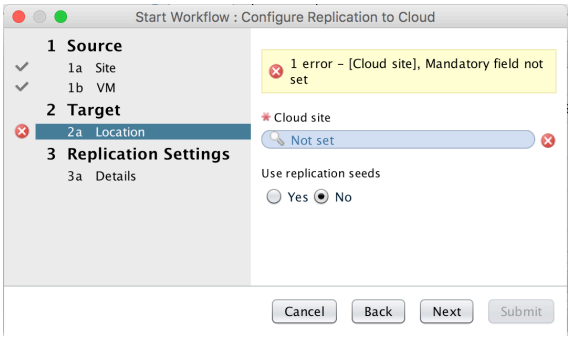


Figure 52. Browse for Cloud Target

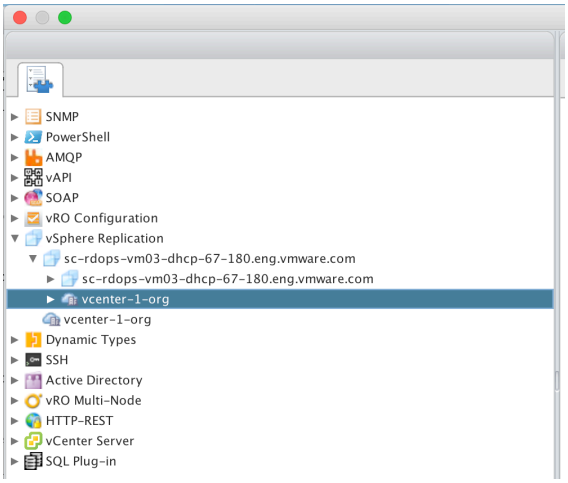
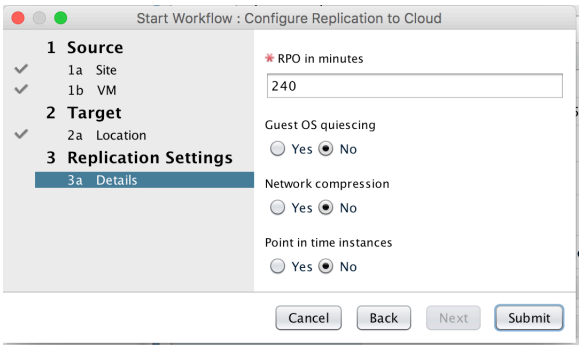


Figure 53. Select Cloud Target

This selection can be a bit confusing. Select the virtual data center that is paired with the VM defined in the tenant vCenter replication appliance. It is nested under the tenant's vSphere Replication appliance. The other **vcenter-1-org** node in the preceding screenshot represents the replication appliance defined by the standalone Organization / virtual data center at the provider. The vSphere Replication plug-in is configured to point to both endpoints.

6. Select **Replication Settings**.

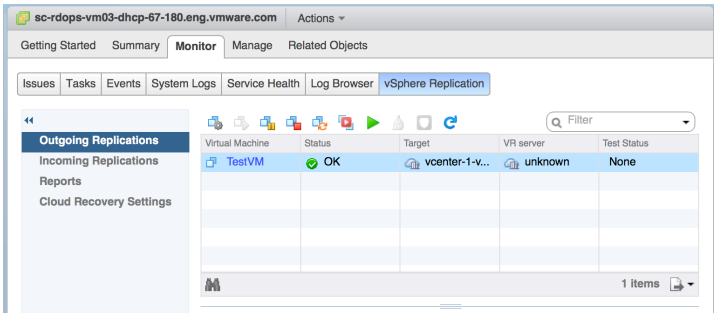
Figure 54. Specify Replication Settings



7. Click **Submit** to execute the workflow.

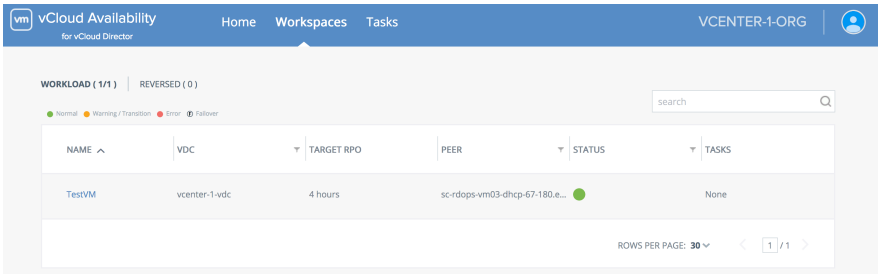
   When the workflow completes successfully, the replication is visible in the tenant vSphere Web Client.

Figure 55. vCenter Client Replication Monitoring



The same information is visible in the vCloud Availability for vCloud Director portal running on the Cloud.

Figure 56. vCloud Availability for vCloud Director Portal Workspace Detail



8.4 Run Test Recovery at the Cloud Site

8.4.1 Prerequisites

The following are prerequisites to running test recovery at the cloud site:

- A virtual machine must be replicated to the Cloud.
- A standalone organization must be added to the vRealize Orchestrator inventory to represent the cloud target.

The following object must exist in the vRealize Orchestrator inventory:

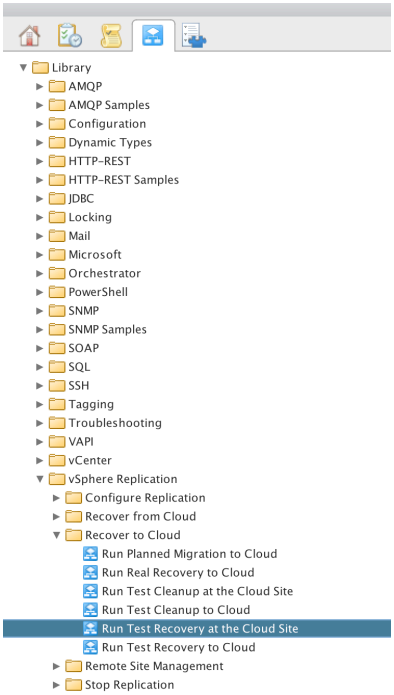
- Workflow input—A defined vCloud Director organization and replication-enabled VDC

This workflow runs a test failover at the provider site. It does not require a connection to the tenant vCenter.

8.4.2 Workflow Execution Steps

1. Select the **Run Test Recovery at the Cloud Site** workflow from the Workflow tab in the vRealize Orchestrator client.

   Figure 57. Run Test Recovery at the Cloud Site Workflow



2. Right-click the object and select **Start Workflow** from the context menu.

3. Select the VM to test on the cloud provider site.

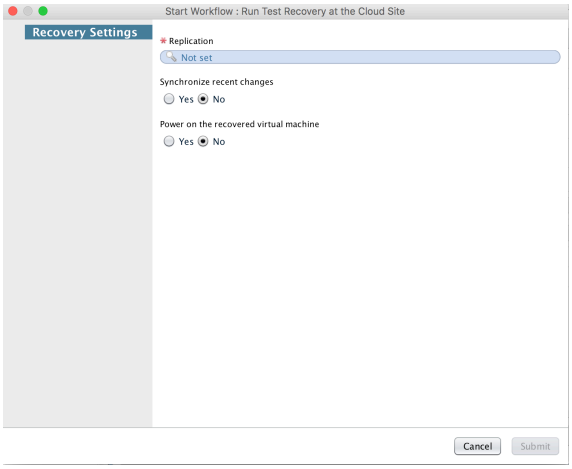


Figure 58. Browse for Virtual Machine

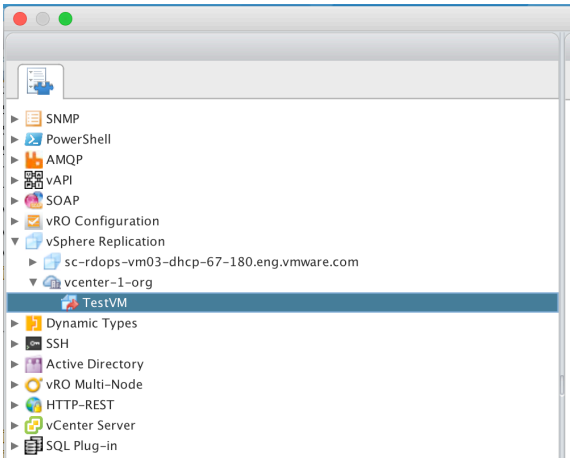
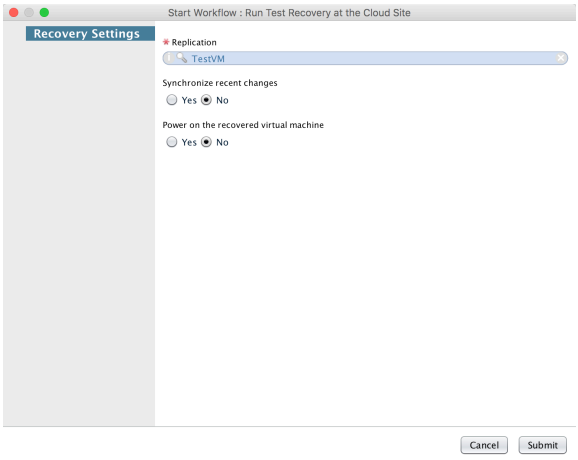


Figure 59. Select Virtual Machine to Test

Note In the preceding figure, the **vcenter-1-org** node is selected. This node was added by the **Register Standalone Organization** workflow, not the on-premises vSphere Replication appliance.

4. Select other options as needed.

Figure 60. Specify Recovery Settings and Start Test



5. Click **Submit** to execute the workflow.

   When the task completes, the virtual machine in vCloud Director should be powered on and available for application testing.

8.5 Protect Virtual Machines in Folder

This workflow provides an example of a custom workflow that was created by reusing actions and a workflow provided the vSphere Replication plug-in.

The workflow configures replication for all virtual machines in a specified folder. This is particularly useful for service providers who organize their tenant's virtual machines in a folder hierarchy.

The workflow can be run on demand or scheduled to run periodically to automatically protect new virtual machines that are added to the folder.

8.5.1 Prerequisites

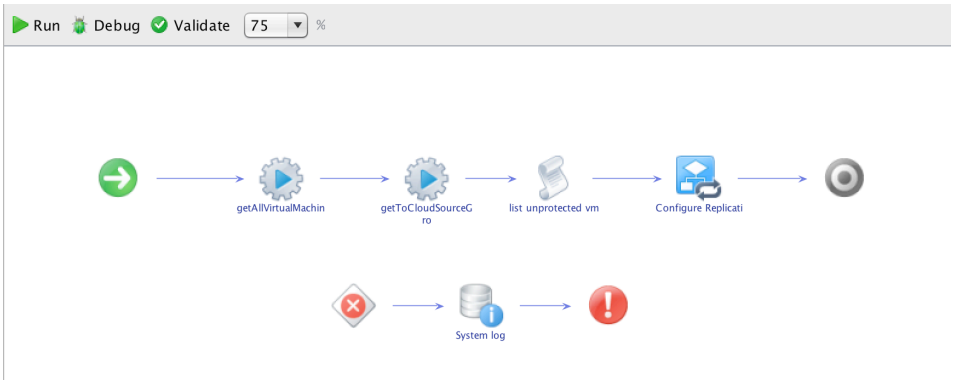
As a prerequisite, the vSphere Replication add-on must have been installed in the vRealize Orchestrator instance.

The following objects must exist in the vRealize Orchestrator inventory:

- Workflow input—A vCloud Director instance
- Workflow input—A vSphere Replication instance

8.5.2 Workflow Overview

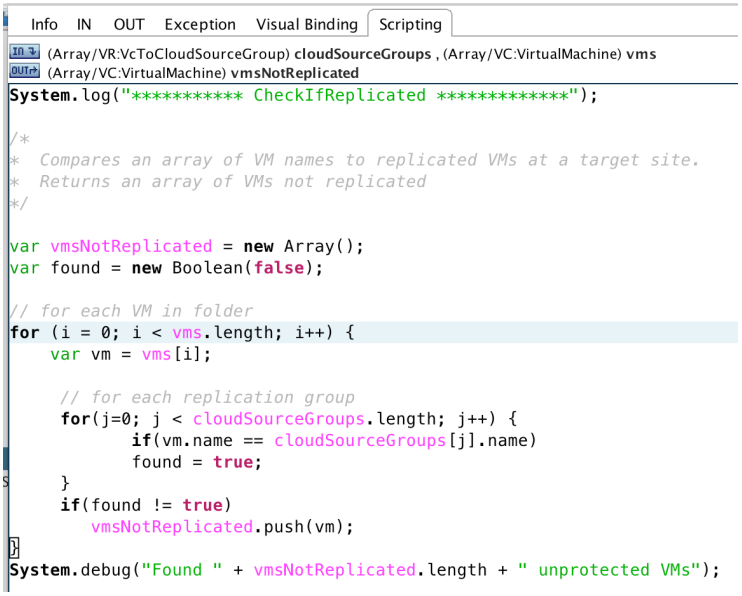
The following screen shot displays the workflow overview.



The workflow includes the following actions:

1. The **getAllVirtualMachines** action retrieves an array of the virtual machines that are contained in the folder specified by an input parameter. This action is provided by the vSphere Replication plug-in.
2. The **getToCloudSourceGroup** action retrieves an array of virtual machines protected at the cloud provider specified by an input parameter. This action is provided by the vSphere Replication plug-in.
3. The **list unprotected vm** element is a JavaScript node that compares the two arrays and determines which virtual machines in the folder are not currently protected. This is a custom addition as shown in the following figure.

Figure 61. CheckIfReplicated



Configure Replication To Cloud is a `ForEach` element that calls the **Configure Replication to Cloud** workflow that was provided by the vSphere Replication plug-in.

Appendix A: vSphere Replication Workflows

This appendix lists the sample workflows included with the vSphere Replication plug-in version 6.1.1.

Workflows marked with an * require only a Cloud connection.

Configure Replication

Workflow	Description
Configure Replication	Configure a virtual machine for replication from this site to another vSphere site.
Configure Replication from Cloud	Configure a virtual machine for replication from a registered Cloud site to this site.
Configure Replication to Cloud	Configure a virtual machine for replication from this site to a registered Cloud site.
Protect Multiple VMs	Configure multiple Virtual Machines for replication.
Reverse a Cloud Replication	Reverse a replication recovered at the cloud site and start copying data from the cloud site to the local site.

Recovery from Cloud

Workflow	Description
Run Planned Migration from Cloud	Migrate a replicated virtual machine from the Cloud to the local site.
Run Real Recovery from Cloud	Recover a virtual machine replicated from the Cloud to this site.
Run Test Cleanup from Cloud	Clean up test recovery results for a replication from the Cloud.
Run Test Recovery from Cloud	Run a test recovery for a replication from the Cloud.

Recovery to Cloud

Workflow	Description
Run Planned Migration to Cloud	Migrate a replicated virtual machine to the Cloud.
Run Real Recovery to Cloud *	Recover a replicated virtual machine at the cloud site. This workflow runs on the cloud site and does not require a source site.
Run Test Cleanup at the Cloud Site *	Clean up test recovery results for a replication to cloud. This workflow runs on the cloud site and does not require a source site.
Run Test Cleanup to Cloud	Cleanup test recovery results for a replication to the Cloud.
Run Test Recovery at the Cloud Site *	Run a test recovery for a replication to the Cloud at the cloud site. This workflow runs on the cloud site and does not require a source site.
Run Test Recovery to Cloud	Run a test recovery for a replication to the Cloud.

Remote Site Management

Workflow	Description
Register Cloud Site	Register login credentials for a cloud site that is paired with a local site.
Register Standalone Org *	Register the URL and credentials for a cloud organization. This workflow does not require the workflow to be paired with a local site.
Register vCenter Site	Register login credentials for a vCenter Server site that is paired with a local site.
Unregister Cloud Site	Delete the login credentials that are stored for a cloud site pairing. This workflow does not break the pairing.
Unregister Standalone Org *	Delete the URL and credentials that are stored for a standalone cloud organization.

Workflow	Description
Unregister vCenter Site	Delete the login credentials that are stored for a vCenter site pairing. This workflow does not break the pairing.

Stop Replication

Workflow	Description
Stop Replication	Stop replicating a virtual machine to another vSphere site.
Stop Replication from Cloud	Stop replicating a virtual machine from the Cloud to a local site.
Stop Replication to Cloud	Stop replicating a virtual machine to the Cloud.

Appendix B: Accessing vCloud Availability for vCloud Director Using the HTTP-REST Plug-In

The vSphere Replication plug-in is typically used to perform orchestration actions against vCloud Availability for vCloud Director. But it also possible to access the vCloud Availability for vCloud Director API using the vRealize Orchestrator REST Plugin.

This appendix provides an overview of how to configure the HTTP-REST plug-in to access vCloud Availability for vCloud Director.

The vSphere Replication plug-in provides access to only a subset of the total vCloud Availability for vCloud Director API. With the HTTP-REST plug-in, it is possible to access the complete API.

This might be needed depending on the desired automation. For example, if you want an orchestration to perform operations on a placeholder vApp that represents a replicated virtual machine, the generated name of the vApp is not available through the vSphere Replication plug-in. Using the HTTP-REST plug-in, the placeholder vApp name can be retrieved and then operations can be performed against the vApp on the vCloud Director server using the vCloud Director plug-in.

Plug-In Installation

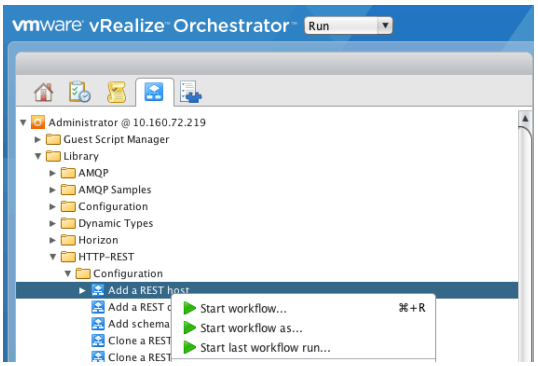
The HTTP-REST plug-in is included with vRealize Orchestrator. No installation of the plug-in is required.

Figure 62. HTTP-REST Plug-In in vRealize Orchestrator Inventory

Add a vCloud Director Rest Host to the vRealize Orchestrator Inventory

1. On the workflow tab in the vRealize Orchestrator client, expand the HTTP-REST folder, right-click the **Add a REST host** workflow, and select **Start workflow**.

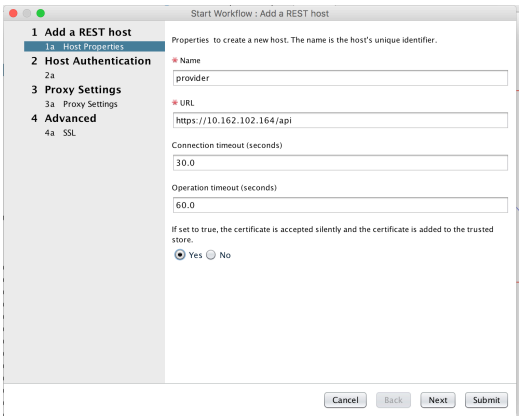
   Figure 63. Add a Rest Host Workflow in vRealize Orchestrator Java Client



2. Enter a name and the HTTPS URL for the target vCloud Director instance as shown in the following screen shot.

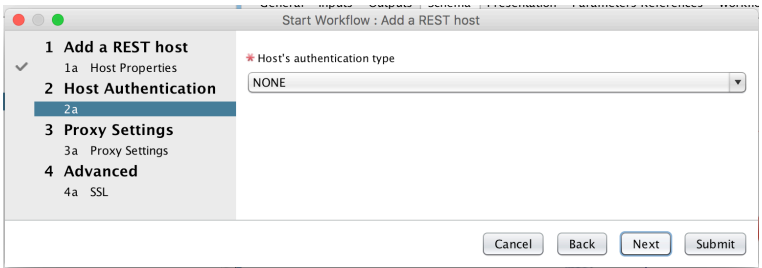
   Note Add the /api suffix to the end of the vCloud Director URL as shown in the following screen shot.

   Figure 64. Rest Host Connection Properties



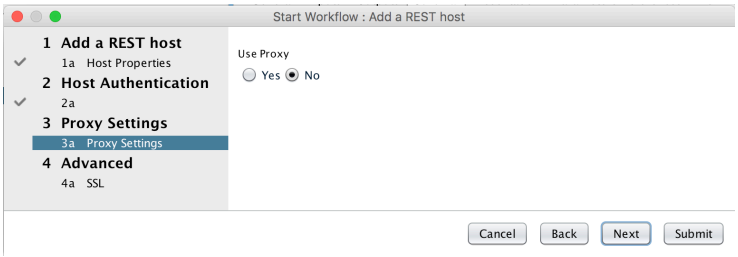
3. Select **NONE** for host authentication. Authentication will be configured in a later step.

   Figure 65. Select Host Authentication Type



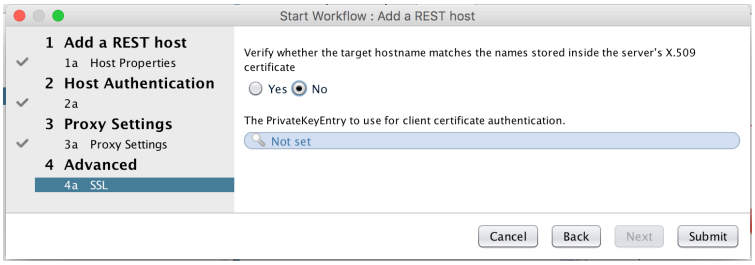
4. Select **No** for **Use Proxy** unless your configuration requires a proxy for internet access.

Figure 66. Host Proxy Setting



5. Select **No** verify target host name if your vCloud Director certificates are self-signed. Otherwise, select **Yes**.

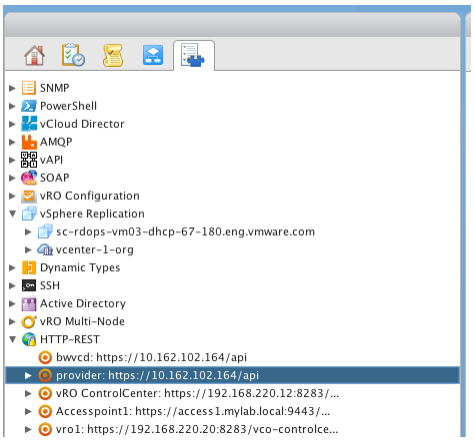
Figure 67. SSL Settings



Click **Submit** to run the workflow.

6. Verify that the workflow execution succeeds. A new HTTP-REST host node should appear under the vRealize Orchestrator inventory tab.

Figure 68. New REST Host in vRealize Orchestrator Inventory

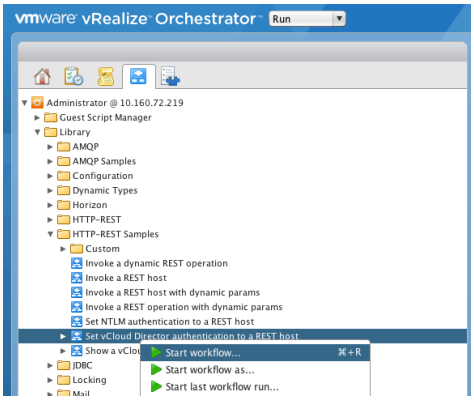


Setup vCloud Director Rest Host Automatic Authentication

The REST plug-in manages the vCloud Director login and maintains an active session. The REST plug-in automatically retrieves and stores the `x-vcloud-authorization` session token.

1. On the workflow tab in the vRealize Orchestrator client, expand the **HTTP-REST Samples** folder, right-click the **Set vCloud Director authentication to a REST host** node, and select **Start Workflow**.

   Figure 69. Set vCloud Director Authentication Workflow



2. In the Start Workflow window, perform the following steps:

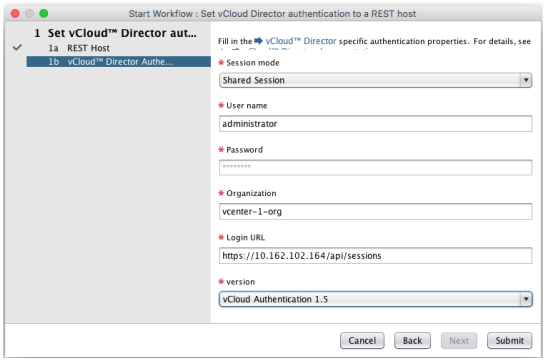
   a. Select **Shared Session** for session mode.

   b. Enter vCloud Director credentials, including user name, password, and vCloud Director organization name.

   c. Enter the vCloud Director login URL, including the `/api/sessions` suffix.

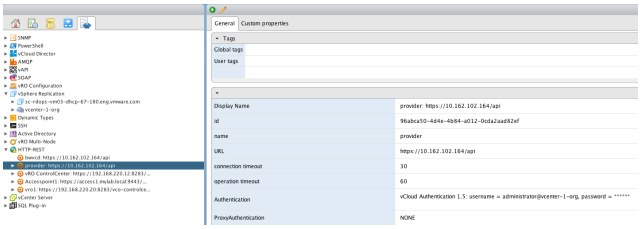
   d. Click **Submit** to execute the workflow.

   Figure 70. Enter vCloud Director Login Credentials



A new value should be visible in the **Authentication** property of the HTTP-Host as shown in the following screen shot.

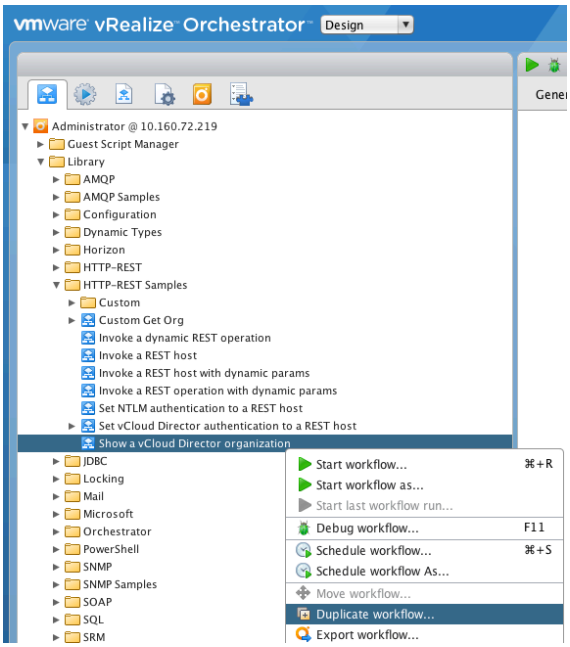
Figure 71. REST Host with Updated Authentication Property



Duplicate a Workflow to Test the Configuration

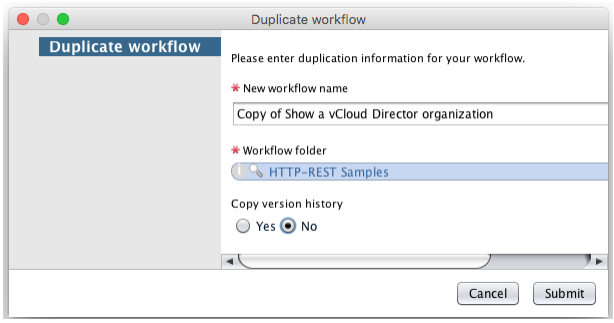
1. Right-click the **Show a vCloud Director organization** workflow node and select the **Duplicate workflow** menu item.

Figure 72. Duplicate Workflow Using Context Menu Action



2. Enter a name for the new workflow.

Figure 73. Supply New Workflow Name



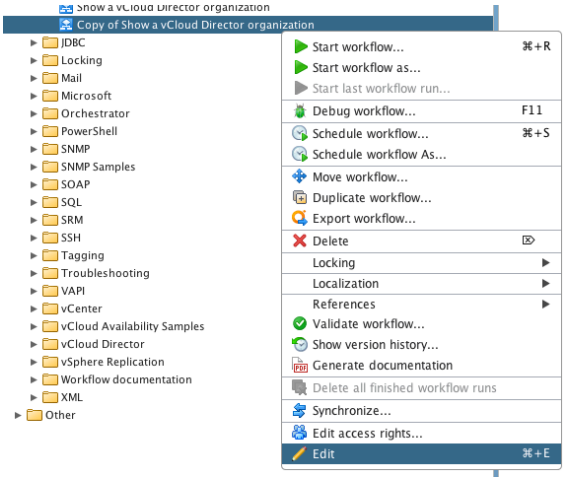
Modify the Workflow and Run the Test

An execution of the new workflow as defined will fail unless it is modified. An **invalid accept header** error will be raised because a valid vCloud Director accept header is not supplied with the GET request.

In the following steps, the script is modified to include the required Accept header.

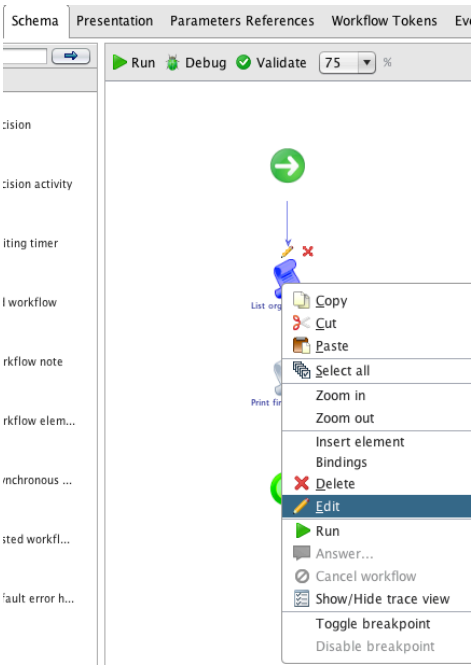
1. Edit the new workflow.

Figure 74. Edit Workflow



2. Select the Schema tab, right-click the **List organizations script** node, and select **Edit**.

Figure 75. Edit Script Action



3. Replace the existing script lines with the following lines.

Note `vcloud_host` is misspelled in the original workflow. Use the following input:

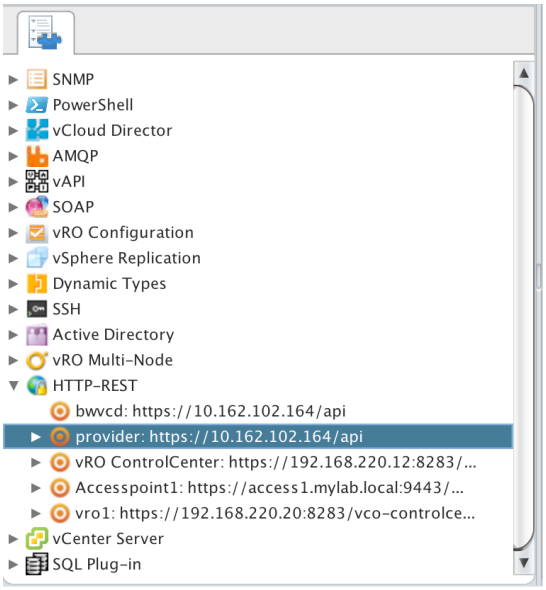
```
var request = vlcoud_host.createRequest("GET", "/org", null);
request.setHeader("Accept", "application/*+xml;version=9.0;vr-
version=3.0");
var response = request.execute();
org_list = response.contentAsString;
System.log(org_list);
```

4. Click **Save** to save the changes.
5. Run the script by clicking **Run**.

Figure 76. Run Action in vRealize Orchestrator Java Client

6. Select the newly created REST host.

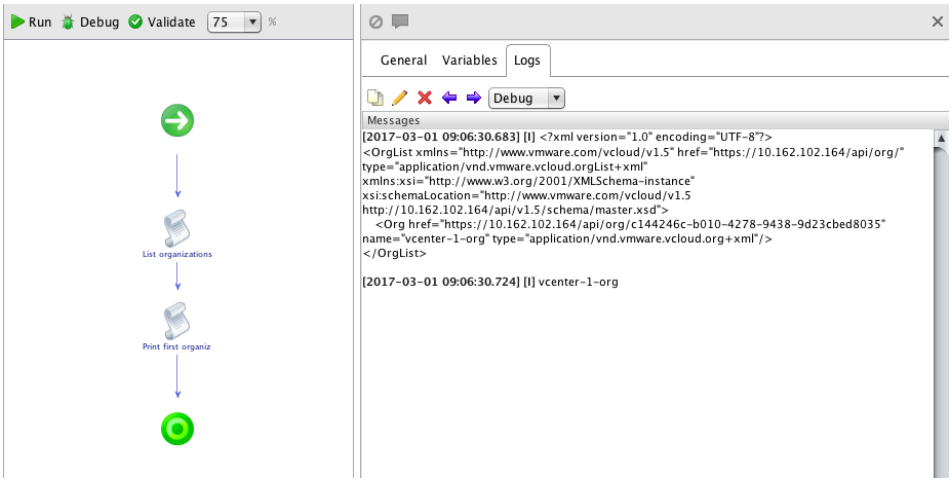
Figure 77. Selecting a REST host



7. Click **Submit**.

The Logs tab should display the results, showing the successful retrieval of the <OrgList> data, as shown in the following screen shot.

Figure 78. Rest Call Workflow Output



This output validates that the HTTP host is successfully configured and an authenticated user can retrieve organization details.

Appendix C: Installing the vRealize Orchestrator vSphere Web Client Extension

Prerequisites

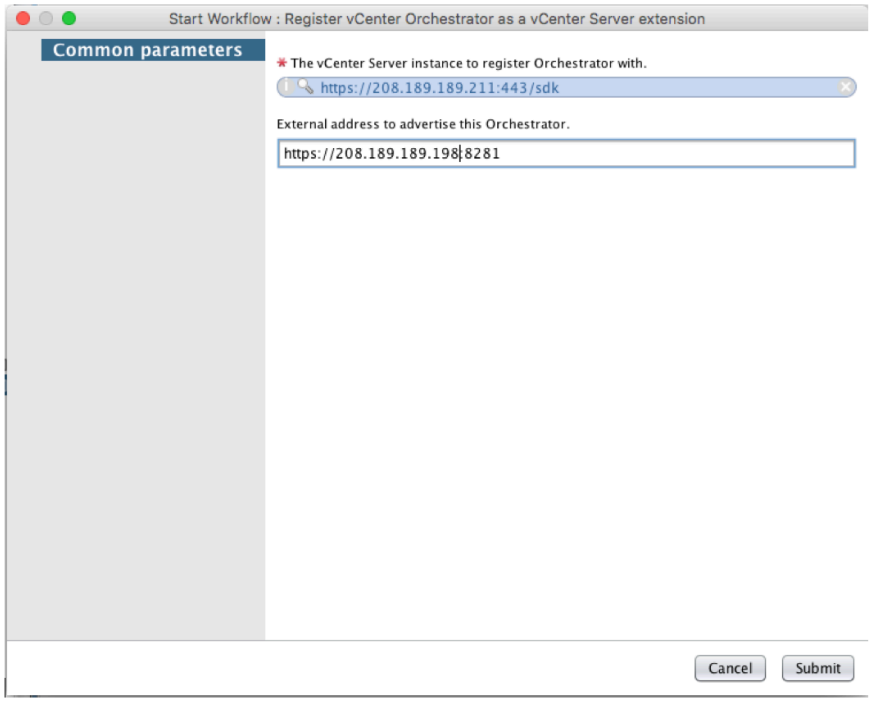
- vRealize Orchestrator Appliance (7.0.1 or 7.2) deployed.
- vSphere authentication provider configured in control center.
- The vCenter Server node has been registered with vRealize Orchestrator by running the **Add vCenter Server instance** workflow.

Setup

To install the extension, execute the following workflow:

1. Register vRealize Orchestration as a vCenter extension.
2. Select the vCenter Server from the vRealize Orchestrator inventory and enter the URL of the vRealize Orchestrator appliance.

   Figure 79. Registering vRealize Orchestrator as vCenter Extension



3. When the workflow successfully completes, log out from vCenter and log in again. You should see the vRealize Orchestrator user interface.

Troubleshooting the vRealize Orchestrator Extension

If the vRealize Orchestrator extension does not appear after clicking the desktop icon, perform the steps in this section.

Step 1: Validate the Extension is Registered

1. Access the mob browser for the vCenter Server.

   For example https://10.192.48.121/mob/

2. Log in using the vCenter administrator credentials.
3. Select the **content** link.
4. Select the **ExtensionManager** link.

   The list should contain an array named **extensionList**.

5. Check the array for an entry named **extensionList["com.vmware.vco"]**.
6. Click the **com.vmware.vco** link.
   - If it does not appear in the list, the extension has not been registered. Try running the **Register vRO as a vCenter extension** again.
   - If the entry does appear in the list, click the **client** link.

This URL must point to a zip file located on the vRealize Orchestrator server. For example, https://208.189.189.211:8281/vco/vsphere-web-client/vco-plugin.zip.

Try pasting the URL into a browser to confirm the extension is available at the URL.

If the URL is incorrect, either run the register extension again and set the external address for vRealize Orchestrator, including the HTTPS protocol, address, and port 8281, or execute the update method in the mob browser to update the URL.

Step 2: Validate Extension is Downloaded

When vSphere Web Client is opened, it enumerates all registered vCenter extensions and tries to download the plug-ins to these extensions.

1. Log in to the vCenter appliance and validate that the extension is downloaded to the following folder on vCenter appliance:

   ```
   /etc/vmware/vsphere-client/vc-packages/vsphere-client-
   serenity/com.vmware.vco-{version}
   ```

2. Check Web client main log file `vsphere_client_virgo.log`, looking for some issues related to operations with this URL.

Step 3: Disable IPv6

1. Log into the vRealize Orchestrator appliance as a **root**.
2. Disable IPv6:

   ```
   sudo sh -c 'echo 1 > /proc/sys/net/ipv6/conf/eth0/disable_ipv6'
   service network restart
   service vco-server restart
   ```

3. Log out from the vSphere Web Client and log in again.