Using VMware vRealize Orchestrator Plug-In for Horizon

VMware Horizon 2106

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

Using VMware vRealize Orchestrator Plug-In for VMware Horizon 6

1 Introduction to vRealize Orchestrator Plug-in for Horizon 7

Role of vRealize Orchestrator Plug-in for Horizon 8

vRealize Orchestrator Plug-in for Horizon Functionality 8

vRealize Orchestrator Plug-in for Horizon Architecture 9

vRealize Orchestrator Plug-in for Horizon Security Model 10

Using Personas to Manage Workflows Across Distributed Organizations 11

2 Installing and Configuring vRealize Orchestrator Plug-in for Horizon 12

Functional Prerequisites for vRealize Orchestrator Plug-in for Horizon 12

Install or Upgrade vRealize Orchestrator Plug-in for Horizon 13

Configure the Connection to a Pod in VMware Horizon 15

Updating Pod Connection Information 16

Configure the App Volumes Server 16

Assigning Delegated Administrators to Desktop and Application Pools 17

Create a Delegated Administrator Role in vSphere Web Client 18

Provide Access Rights to the vRealize Orchestrator Plug-in for Horizon Workflows 20

Assign Delegated Administrators to Pools 21

Configuration Tasks for Self-Service Workflows and Unmanaged Machines 22

Best Practices for Managing Workflow Permissions 23

Set a Policy for De-Provisioning Desktop Virtual Machines 24

3 Using vRealize Orchestrator Plug-in for Horizon Workflows 26

Access the vRealize Orchestrator Plug-in for Horizon Workflow Library 26

vRealize Orchestrator Plug-in for Horizon Workflow Library 27

vRealize Orchestrator Plug-in for Horizon Workflow Reference 28

Add Managed Machines to Pool 28

Add Unmanaged Machines to Pool 28

Add Users to an App Pool 29

Add Users to App Pools 29

Add Users to a Desktop Pool 29

Advanced Desktop Allocation 30

Application Entitlement 30

Assign User 31

Desktop Allocation 31

Desktop Allocation for Users 31

Desktop Assignment 32

Desktop Entitlement 32

Desktop Recycle 32

Duplicate a Desktop Pool 33

Global Entitlement Management 33

Port Pool to vCAC 33

Register Machines to Pool 33

Remove Users From Application Pool 34

Remove Users From Desktop Pool 34

Self-Service Advanced Desktop Allocation 34

Self-Service Desktop Allocation 35

Self-Service Desktop Recycle 36

Self-Service Release Application 36

Self-Service Request Application 36

Self Service Request Application Stack 37

Session Management 37

Set Maintenance Mode 37

Unassign User 37

Update App Pool Display Name 38

Update Desktop Pool Display Name 38

Update Desktop Pool Min Size 38

Update Desktop Pool Spare Size 38

Syntax for Specifying User Accounts in the Workflows 38

4 Making the Workflows Available in vSphere Web Client and vRealize Automation 40

Exposing VMware vRealize Orchestrator Plug-in for Horizon Workflows in vSphere Web Client 40

Bind vSphere Web Client Workflows to Specific Pods and Pools in vRealize Orchestrator 40

Create Localized Versions of a Workflow for vSphere Web Client 42

Exposing vRealize Orchestrator Plug-in for Horizon Workflows in vRealize Automation 43

Create Business Groups for Delegated Administrators and End Users 44

Create Services for Delegated Administrators and End Users 45

Create Entitlements for Delegated Administrators and End Users 45

Bind vCAC Workflows to a vCAC User 46

Configure Output Parameters for vCAC Workflows 48

Configure the Catalog Item for the Workflow 49

5 Making Desktop and Pool Actions Available in vRealize Automation 51

Export Action Item Icons from vRealize Orchestrator 51

Import Desktops and Pools as Custom Resources 52

Import Actions for Desktop and Pool Items 53

Import Workflows for Desktop and Pool Management 55

Import the Self-Service Desktop Allocation Workflow 56

Import the Self-Service Advanced Desktop Allocation Workflow 57

Import the Advanced Desktop Allocation Workflow 58

Import the Assign an AppStack to User Workflow 59

Import the Self-Service Remote Application Workflow 60

Import the Port Pool to vCAC Workflow 60

Entitle Users to Action Items 62

Import Action Icons into vRealize Automation 63

6 Creating Machines and Managing Pools in vRealize Automation 64

Prerequisites for Creating Machines in vRealize Automation 64

Create Templates and Blueprints for Adding Machines to Desktop Pools 65

Use Machine Blueprints to Create and Add Desktops to Pools 67

Configure a Machine Blueprint Service for Advanced Desktop Allocation 68

Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users 70

Deleting Machines Provisioned by vRealize Automation 73

7 Working with Unmanaged Machines 75

Prerequisites for Adding Unmanaged Machines to Pools 75

Adding Physical Machines and Non-vSphere Virtual Machines to Pools 77

Configure a Physical Machine for an Unmanaged Pool 77

Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines 80

Run Workflows to Add Physical Machines as PowerShell Hosts 81

Using VMware vRealize Orchestrator Plug-In for VMware Horizon

This document, *Using VMware vRealize Orchestrator Plug-In for Horizon*, describes how to set up and use VMware vRealize® Orchestrator™ Plug-in for VMware Horizon®. With this plug-in, IT organizations can use VMware vRealize Automation™ to automate the provisioning of remote desktops and published applications in VMware Horizon.

Intended Audience

The information in this document is intended for anyone who needs to install and configure the plug-in, or who wants to automate and provision remote desktops and published applications by using the workflow library. This document is written for experienced users that are familiar with virtual machine technology, vRealize Orchestrator workflow development, and VMware Horizon.

Introduction to vRealize Orchestrator Plug-in for Horizon

1

VMware vRealize Orchestrator Plug-in for Horizon enables interaction between vRealize Orchestrator and VMware Horizon. You can use the plug-in to expand the settings and methods for provisioning remote desktops and published applications.

The plug-in contains a set of standard workflows that enable automation, self-service by request and approval, and scalable delegated administration across multi-tenant or highly distributed environments. You can also use these predefined workflows to create custom workflows.

This document describes workflows that provide predefined automated tasks that accomplish basic goals that are ordinarily performed in Horizon Console or other VMware interfaces. Horizon administrators can increase IT efficiency by delegating access to these workflows to delegated administrators and end users.

For end-user enablements, vRealize Orchestrator Plug-in for Horizon integrates with vRealize Automation to provide self-service access to remote desktops and published applications. If you integrate the plug-in workflows with the request and approval processes that are built into the vRealize Automation service catalog, end users can refresh their own remote desktops. End users can make requests that follow a standardized and auditable process. These requests can result in immediate action, or they can be directed for administrative approval. For remote desktodep environments where virtual machines must support rapid change and reuse, end users can provision desktops for themselves, and de-provision, or recycle, remote desktops to reduce resource and capacity waste.

vRealize Orchestrator Plug-in for Horizon provides an organized and manageable service catalog of functions that is entitled to users and groups. By automating and distributing tasks for delegated administration, you can reduce the need for email correspondence and exception handling. Requests are routed into processes that are predefined and flagged for approval only if a justification is required.

This chapter includes the following topics:

- Role of vRealize Orchestrator Plug-in for Horizon
- vRealize Orchestrator Plug-in for Horizon Functionality
- vRealize Orchestrator Plug-in for Horizon Architecture
- vRealize Orchestrator Plug-in for Horizon Security Model

- Using Personas to Manage Workflows Across Distributed Organizations

Role of vRealize Orchestrator Plug-in for Horizon

To install and configure vRealize Orchestrator Plug-in for Horizon, you use the vRealize Orchestrator configuration interface. To run and create workflows and access the plug-in API, you use the vRealize Orchestrator client.

vRealize Orchestrator Plug-in for Horizon is powered by vRealize Orchestrator. vRealize Orchestrator is a development and process-automation platform that provides a library of extensible workflows to manage the VMware vCenter® infrastructure and other technologies.

vRealize Orchestrator Plug-in for Horizon Functionality

vRealize Orchestrator Plug-in for Horizon provides automation, self-service, and delegated administration for VMware Horizon environments. End users can perform self-service functions. Delegated administrators can perform provisioning functions on behalf of end users.

Table 1-1. vRealize Orchestrator Plug-in for Horizon Functions

Category	Functions
Self-service	All self-service functions are provided through vRealize Automation. ■ Self-provision and de-provision, or recycle, machines in existing desktop pools. ■ Self-service request and entitlement for applications and desktops. ■ Self-service management of desktops, including refresh, restart, recycle, log out, and more. ■ Self-service management of approving and automatically provisioning approved application requests. ■ Self-service request for published applications. ■ Self-service request for a VMware App Volumes® application stack.
Machine provisioning	■ Provision a machine into an existing desktop pool on behalf of an end user. ■ Provision multiple machines for multiple users. ■ Provision from vRealize Automation to create either VMware Horizon or vRealize Automation machines. ■ De-provision a machine on behalf of an end user and preserve the persistent disk, if a persistent disk exists. ■ Perform maintenance operations on machines.

Table 1-1. vRealize Orchestrator Plug-in for Horizon Functions (continued)

Category	Functions
Pool maintenance	■ Perform recompose operations on one or more pools. ■ Perform pool-level functions and day-2 management operations on machines through vRealize Automation by using action buttons such as Manage Assignment, Manage Session, Refresh, and Recompose. ■ Add managed and unmanaged virtual machines to manual desktop pools. ■ Add vRealize Automation IaaS blueprint-provisioned machines to manual pools. ■ Add physical machines to manual unmanaged desktop pools. ■ Allow modification of the minimum number of machines in a desktop pool, pool display name, and number of powered-on machines. ■ Perform duplication of desktop pools.
Assignment and entitlement	■ Add users to and remove users from global entitlements in a Cloud Pod Architecture environment.

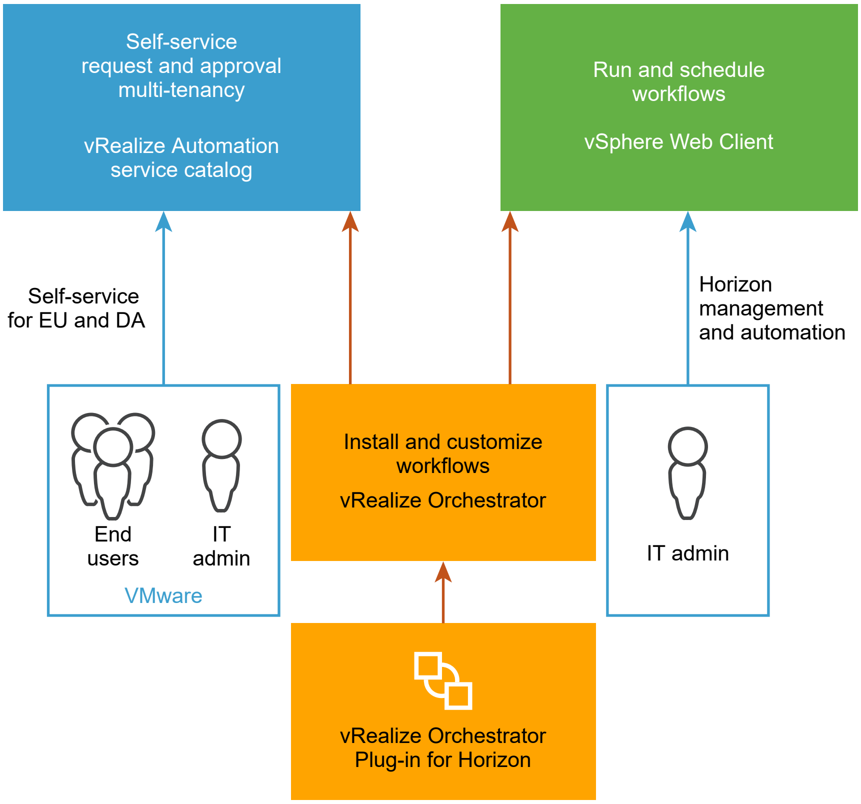
vRealize Orchestrator Plug-in for Horizon Architecture

vRealize Orchestrator and vRealize Automation provide the architecture that supports the functions of vRealize Orchestrator Plug-in for Horizon.

vRealize Orchestrator plug-ins enable a consistent automation between the software environment in which the workflows run and the products with which the workflows interact. With vRealize Orchestrator Plug-in for Horizon, workflows can be exposed natively to delegated administrators through VMware vSphere® Web Client and the vRealize Automation service catalog. You can customize and configure the workflows in the vRealize Orchestrator client.

The following diagram illustrates the architecture of vRealize Orchestrator Plug-in for Horizon.

Figure 1-1. Architecture of vRealize Orchestrator Plug-in for Horizon



vRealize Orchestrator Plug-in for Horizon Security Model

vRealize Orchestrator Plug-in for Horizon uses a trusted account security model. The administrator provides the credentials to the initial configuration between a pod and the plug-in. That trusted account is the security context that all workflows use between vRealize Orchestrator and VMware Horizon.

Additional levels of permissions also restrict which users can see and edit the workflows within vRealize Orchestrator. All vRealize Orchestrator Plug-in for Horizon workflows must be explicitly configured for execution. Access to the workflows requires both the permissions and the vRealize Orchestrator client interaction with the client.

In addition, the third level of security is an access layer between where the workflows run in vRealize Orchestrator and where they are exposed to delegated administrators and end users in vSphere Web Client and vRealize Automation.

Administrators use the VMware vCenter® Single Sign-On implementation to enable users and groups to run workflows within vSphere Web Client. Administrators use the service catalog and entitlement mechanisms within vRealize Automation to manage which workflows are exposed to specific users and groups.

Using Personas to Manage Workflows Across Distributed Organizations

The administrator, delegated administrator, and end-user personas describe the roles and privileges available to individuals and groups when you implement vRealize Orchestrator Plug-in for Horizon. Organizations can further divide these primary roles into geographic and functional areas.

Administrator Persona

The administrator persona encompasses the typical administrator role. Responsibilities include the installation, configuration, and assignment of other personas to roles and privileges. This persona is responsible for products, configuration, and single sign-on (SSO) implementation. The administrator decides which users can access the workflows and whether to expose each workflow through vSphere Web Client or vRealize Automation. When making decisions about workflows, the administrator considers which mechanisms offer the greatest organizational efficiency.

Delegated Administrator Persona

The administrator delegates the role and responsibilities of the delegated administrator. The delegated administrator can perform actions on specific desktop and application pools. Delegated administrators cannot change the scope of responsibilities for which they have been granted access. The functions granted to the delegated administrator can include complex tasks, such as provisioning multiple virtual machine desktops, and simple tasks, such as resetting desktops. Delegated administrators can act on behalf of multiple users. This power is key to enabling administrative efficiency.

End User Persona

End users always act on their own behalf. End-user tasks are focused on a narrow set of resources, such as individual desktops or applications. Self-service workflows enable the automation of repetitive tasks and empowerment of end users.

Installing and Configuring vRealize Orchestrator Plug-in for Horizon

2

Installing vRealize Orchestrator Plug-in for Horizon is similar to installing other vRealize Orchestrator plug-ins. Configuring the plug-in involves running various configuration workflows to connect to VMware Horizon components, and configuring roles and permissions.

This chapter includes the following topics:

- Functional Prerequisites for vRealize Orchestrator Plug-in for Horizon
- Install or Upgrade vRealize Orchestrator Plug-in for Horizon
- Configure the Connection to a Pod in VMware Horizon
- Configure the App Volumes Server
- Assigning Delegated Administrators to Desktop and Application Pools
- Configuration Tasks for Self-Service Workflows and Unmanaged Machines
- Best Practices for Managing Workflow Permissions
- Set a Policy for De-Provisioning Desktop Virtual Machines

Functional Prerequisites for vRealize Orchestrator Plug-in for Horizon

vRealize Orchestrator Plug-in for Horizon acts as middleware between VMware Horizon, vRealize Orchestrator, vRealize Automation, and App Volumes Server. To install and use vRealize Orchestrator Plug-in for Horizon, your system must meet certain functional prerequisites.

VMware Horizon

You must have access to a Connection Server instance in your VMware Horizon implementation. VMware Horizon works with vRealize Orchestrator Plug-in for Horizon 1.5.

For information about setting up VMware Horizon, see the VMware Horizon documentation.

vRealize Orchestrator

Verify that you have a running instance of vRealize Orchestrator. You can log in to the vRealize Orchestrator configuration interface at http://*orchestrator_server*:8283. vRealize Orchestrator Plug-in for Horizon 1.5 works with vRealize Orchestrator 7.4 and later.

For information about setting up vRealize Orchestrator, see the *Installing and Configuring VMware vRealize Orchestrator* document.

vRealize Automation

You must have access to a vRealize Automation server. vRealize Orchestrator Plug-in for Horizon 1.5 works with vRealize Automation 7.4 and later. The embedded vRealize Orchestrator server packaged with vRealize Automation 7.4 and later is compatible with this plug-in. Alternatively, you can install the plug-in on an external vRealize Orchestrator server.

For information about setting up vRealize Automation, see the *Installing and Upgrading vRealize Automation* document.

App Volumes Server

You must have access to an App Volumes Server instance before you can use the Self Service Request Application Stack workflow. vRealize Orchestrator Plug-in for Horizon 1.5 works with App Volumes Server 2.12.1 and later. Verify that you have the credentials of a user that has the App Volumes Administrators role.

For information about installing and setting up an App Volumes Server instance, see the *VMware App Volumes Installation Guide* document.

vCenter Server and vCenter Single Sign-On

Verify that you have access to an instance of VMware vCenter Server® 6.5, or vCenter Server 6.0 or later, and that you are using VMware vCenter® Single Sign-On 2.0 or later.

For information about setting up vCenter Server, see the *vSphere Installation and Setup* document.

Install or Upgrade vRealize Orchestrator Plug-in for Horizon

Installing or upgrading vRealize Orchestrator Plug-in for Horizon involves downloading the latest installer file and using the vRealize Orchestrator Configuration user interface to upload and install the plug-in.

This topic provides specific guidance for installing vRealize Orchestrator Plug-in for Horizon. The procedure for installing vRealize Orchestrator Plug-in for Horizon is similar for all plug-ins. For general plug-in installation, update, and troubleshooting information, see the vRealize Orchestrator documentation.

Prerequisites

- Verify that the functional prerequisites are met. See Functional Prerequisites for vRealize Orchestrator Plug-in for Horizon .
- Verify that you have the URL for downloading the vRealize Orchestrator Plug-in for Horizon installation file.
- Verify that vRealize Orchestrator is set up and configured to work with vCenter Single Sign-On. For information, see the *Installing and Configuring VMware vRealize Orchestrator* document.
- Verify that you have credentials for an account that has permission to install vRealize Orchestrator Plug-in for Horizon and to authenticate through vCenter Single Sign-On.
- If appropriate for your version of vRealize Orchestrator, verify that VMware vRealize Orchestrator client is installed and that you can use Administrator credentials to log in to it.

Procedure

1 Download the vRealize Orchestrator Plug-in for Horizon installer file to a location that is accessible from the vRealize Orchestrator appliance or service.

The installer filename is `o11nplugin-horizon-`*`1.5.0-xxxxxxx`*`.vmoapp`, where *xxxxxx* is the build number.

2 Open a browser and start the vRealize Orchestrator Configuration interface.

An example of the URL format is `https://`*`server.mycompany`*`.com:8283`.

3 To upload the plug-in installer file, use the vRealize Orchestrator Configuration interface.

a Click the **Manage Plugin** icon.

b Upload the plug-in installer file

The file must be in `.vmoapp` format.

4 In the Install a Plugin pane, when prompted, accept the license agreement.

Important If you are upgrading, a message appears after the plug-in is installed, for example, `Horizon (1.5.0 build `*`xxxxxxx`*`) Plug-in with same name was already installed (1.4.0 build `*`xxxxxxx`*`): overwriting existing plug-in.`

5 Go to the **Enabled plug-ins installation status** section and confirm that `Horizon 1.5.0.`*`xxxxxxx`* is listed.

xxxxxx is the build number. A status message appears for the installation or upgrade.

Type of Installation	Message
New installation	`Plug-in will be installed at next server startup.`
Upgrade	`Will perform installation at next server startup.`

6 Restart the vRealize Orchestrator Server service.

7 Wait for the vRealize Orchestrator Plug-in for Horizon installation to finish.

   The installation can take several minutes.

8 Start the vRealize Orchestrator Configuration interface again, click the **Plug-ins** item, and verify that the status changed to `Installation OK`.

9 If you are upgrading, delete the vCAC61 folder from the **Workflows** tab.

   This folder is in **Library > Horizon > Workflows**.

   After the upgrade, the vCAC61 folder is empty, so you can delete it. You cannot delete the vCAC60 folder because it contains published items.

   Important Do not use any of the workflows in the vCAC60 folder. vRealize Orchestrator Plug-in for Horizon 1.5 does not support vRealize Automation 6.0.

What to do next

Log in to vRealize Orchestrator and use the **Workflow** tab to navigate through the library to the `Horizon` folder. You can now browse through the workflows provided by vRealize Orchestrator Plug-in for Horizon.

Continue to perform the configuration tasks. See Configure the Connection to a Pod in VMware Horizon.

Configure the Connection to a Pod in VMware Horizon

You run the Add View Pod workflow to provide the appropriate credentials for all workflow operations that the Connection Server instance performs.

Prerequisites

- Verify that the fully qualified domain name of the Connection Server instance can be resolved from the machine where the vRealize Orchestrator server is running.
- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have the credentials of a user that has the Administrators role in Horizon Console. The users and groups that have the Administrators role were specified in Horizon Console when the Connection Server instance was installed and configured.

Procedure

1 Log in to vRealize Orchestrator as an administrator.

2 Click the **Workflows** view in vRealize Orchestrator.

3 In the workflows hierarchical list, select **Library > Horizon > Configuration > View Pod Configuration** and navigate to the **Add View Pod in Configuration** workflow.

4 Right-click the **Add View Pod in Configuration** workflow and select **Start workflow**.

5 Provide a name for the pod.

6 Provide the fully qualified domain name of the machine on which the Horizon Connection Server instance is installed.

7 Provide the credentials of a user that has the Administrators role in Horizon Console.

8 Verify and accept the SSL certificate information.

9 To run the workflow, click **Submit**.

Results

After the workflow runs, you can click the expander button to see the status.

What to do next

Add a delegated administrator.

Updating Pod Connection Information

If the user credentials for a Connection Server instance change, or if the members of a replicated group of Connection Server instances change, you must run the corresponding workflow in vRealize Orchestrator.

You can navigate to the folder that contains these workflows by using the vRealize Orchestrator Client and selecting **Library > Horizon > Configuration > View Pod Configuration**.

- If the credentials for the Connection Server instance change, run the Update View Pod Credential Configuration workflow.
- If the names of the servers or the number of instances in the pod change, run the Refresh View Pod Connection Server List workflow.

Configure the App Volumes Server

You can optionally run the App Volumes Configuration workflow to provide the appropriate credentials for all workflow operations that the VMware App Volumes™ Server instance performs.

Prerequisites

- Verify that the fully qualified domain name of the App Volumes Server instance can be resolved from the machine where the vRealize Orchestrator server is running.
- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.

- Verify that you have the credentials of a user that has the App Volumes Administrators role. The users and groups that have the App Volumes Administrators role were specified in App Volumes Administrator when the App Volumes Server instance was installed and set up.

Procedure

1 Log in to vRealize Orchestrator as an administrator.

2 Click the **Workflows** view in vRealize Orchestrator.

3 In the workflows hierarchical list, select **Library > Horizon > Configuration > App Volumes Configuration** and navigate to the **Add or Update App Volumes Server** workflow.

4 Right-click the **Add or Update App Volumes Server** workflow and select **Start workflow**.

5 Use the following information to enter values in the form that appears.

Option	Action
HTTP or HTTPS	From the drop-down menu, select which protocol to use based on the App Volumes configuration.
FQDN or IP address	Provide the fully qualified domain name (FQDN) or IP address of the machine on which the App Volumes Server instance is installed.
The Port	Provide the port number to use. The default is `80`.
The Admin user name	Provide the user name of a user that has the Administrators role in VMware Horizon.
The Password	Provide the password for the administrative user that you specified.
The Timeout to Connect	Specify the length of time, in seconds, that is allowed before the connection times out. The default is `0.0`.

6 Click **Submit**.

The App Volumes Server that you specified is added and can now be listed for the vRealize Orchestrator Plug-in for Horizon under the inventory menu.

Assigning Delegated Administrators to Desktop and Application Pools

To delegate responsibilities to delegated administrators, the administrator runs a workflow. If your setup does not already contain a user group that has the permission to register and update vCenter Server extensions, and the permission to run workflows in vRealize Orchestrator, you must first create such a group.

Depending on your current setup, you might have already performed one or both of the first tasks.

Procedure

1 Create a Delegated Administrator Role in vSphere Web Client

  To use delegated administration, you must create a user group that has permission to register and update vCenter Server extensions.

2 Provide Access Rights to the vRealize Orchestrator Plug-in for Horizon Workflows

  After you create a delegated administrators group and assign it permission to perform actions on vCenter Server extensions, you can give the group permission to view and execute workflows in vRealize Orchestrator.

3 Assign Delegated Administrators to Pools

  To set the scope of delegated administration, the administrator runs the Add Delegated Administrator Configuration workflow. For example, a certain delegated administrator might be limited to performing operations on some pools, and a different delegated administrator might be limited to different pools.

What to do next

Restrict permissions to various workflow folders in vRealize Orchestrator.

Create a Delegated Administrator Role in vSphere Web Client

To use delegated administration, you must create a user group that has permission to register and update vCenter Server extensions.

If you have been using vRealize Orchestrator, and have already created users and groups that have permission to register and update vCenter Server extensions, you might not have to perform all the steps described in this topic. For example, if you already have such a group, but the user that manages desktop and application pools is not in the group, you can add that user to the group.

Prerequisites

Verify that you have credentials for logging in to vSphere Web Client as a user that has vCenter Single Sign-On administrator privileges.

Procedure

1 Log in to vSphere Web Client as administrator@vsphere.local, or as another user that has vCenter Single Sign-On administrator privileges.

2 Create a Delegated Administrators group.

   a Browse to **Administration > Single Sign-On > Users and Groups**.

   b Select the **Groups** tab and click the **New Group** icon.

   c Supply a name, such as `Delegated Admins`, and click **OK**.

   The new group appears in the list.

3 Select the group that you created and use the **Group Members** section of the tab to add a delegated administrator user to this group.

   This user must be a member of the domain that includes the Connection Server instance.

4 Create a role that has permission to read vCenter Server extensions.

   a Browse to **Administration > Roles**.

   b On the **Roles** tab, click the **Create role action** icon.

   c Supply a name for the role and select the **Extensions** check box.

   If you expand the **Extensions** item, the **Register extension**, **Unregister extension**, and **Update extension** check boxes are also selected.

   d Click **OK**.

   The new role appears in the list.

5 Add the new role to the group that you created.

   a Go to the vCenter Home page and browse to **vCenter > Inventory Lists > vCenters**.

   b Select the appropriate vCenter Server instance in the left pane, and click the **Manage** tab.

   c On the **Manage** tab, click **Permissions** and click the **Add permission** icon.

   d In the Users and Groups pane, click **Add** and add the group you just created.

   To find the group, select the correct domain.

   The group appears in the list of users and groups in the Add Permission dialog box.

   e In the Assigned Role pane, click the drop-down arrow and select the role you just created.

   In the list of permissions for this role, a check mark appears next to **Extensions**.

   f Click **OK**.

   The group appears on the **Permissions** tab with the role that you assigned.

What to do next

Provide the Delegated Administrators group access to the vRealize Orchestrator Plug-in for Horizon workflows. See Provide Access Rights to the vRealize Orchestrator Plug-in for Horizon Workflows.

Provide Access Rights to the vRealize Orchestrator Plug-in for Horizon Workflows

After you create a delegated administrators group and assign it permission to perform actions on vCenter Server extensions, you can give the group permission to view and execute workflows in vRealize Orchestrator.

If you have been using vRealize Orchestrator and have already created users and groups that have permission to view, inspect, and execute vCenter Server extensions, you might not have to perform the procedure described in this topic.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have created a delegated administrators group and assigned a role that has Extensions permissions in vCenter Server. See Create a Delegated Administrator Role in vSphere Web Client.

Procedure

1. Log in to vRealize Orchestrator as an administrator and select **Design** from the drop-down menu in the upper-left portion of the screen.
2. Right-click the root directory in the left pane and select **Edit access rights**.
3. In the Edit Access Rights dialog box, click **Add access rights**.
4. In the Chooser dialog box, in the **Filter** text box, type the first few letters of the name of the delegated administrators group, and, when the group name appears in the list, select the group.
5. Select the **View** check box, deselect any other check boxes, and click **Select**.

   The group appears in the list in the Edit Access Rights dialog box.
6. Click **Save and close**.

   The group appears on the **Permissions** tab and, in the Rights column, you see that the group has View permissions.
7. Expand the library in the left pane and right-click the `Horizon` folder.
8. Select **Edit access rights** from the context menu and click **Add access rights**.
9. Type the name of the delegated administrators group in the **Filter** text box, select the group in the list, and select the **View**, **Inspect**, and **Execute** check boxes.

10 Click **Select** in the Chooser dialog box and click **Save and close** in the Edit Access Rights dialog box.

   The group appears on the **Permissions** tab and, in the Rights column, you see that the group has View, Inspect, and Execute permissions.

What to do next

Assign the delegated administrators group to specific desktop and application pools. See Assign Delegated Administrators to Pools.

Assign Delegated Administrators to Pools

To set the scope of delegated administration, the administrator runs the Add Delegated Administrator Configuration workflow. For example, a certain delegated administrator might be limited to performing operations on some pools, and a different delegated administrator might be limited to different pools.

Running the Add Delegated Administrator Configuration workflow is required for configuring the vRealize Orchestrator Plug-in for Horizon. At a minimum, the primary administrator must be assigned to the pools. Using this workflow, the administrator has tight control over which pools can have distributed administration and which workflows can be used.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have provided access rights for the delegated administrators group to view and run workflows for vRealize Orchestrator Plug-in for Horizon. See Provide Access Rights to the vRealize Orchestrator Plug-in for Horizon Workflows.
- Verify that a connection has been made to the pod by running the Add View Pod in Configuration workflow. See Configure the Connection to a Pod in VMware Horizon.

Procedure

1 Log in to vRealize Orchestrator as an administrator.

2 Click the **Workflows** view in vRealize Orchestrator.

3 In the workflows hierarchical list, select **Library > Horizon > Configuration > Delegated Admin Configuration** and navigate to the **Add Delegated Administrator Configuration** workflow.

4 Right-click the workflow and select **Start workflow**.

5 Use the following information to enter values in the form that appears.

Option	Action
Horizon View Pod	Select an item from the drop-down menu. Items get added to this list through the Add View Pod in Configuration workflow.
Select Desktop Pool IDs	Click **Not Set** and add one or more pools from the **New value** drop-down menu.
Select Application Pool IDs	Click **Not Set** and add one or more pools from the **New value** drop-down menu.
Add Delegated Administrator user or group?	Select an item from the drop-down menu. You can add users one by one or add a group from Active Directory. **Note** To add a group, you must be using vRealize Orchestrator 6.0.4 or a later release.
Delegated Administrator User/ Group Name	Click **Not Set** and, in the **Filter** text box, enter the name of the user or group you included in the delegated administrators group. **Note** If you add a user name for a delegated administrator and the user name contains any special characters, the workflow will report success, but the delegated administrator configuration will not be added for that user.
Select Global Entitlement	(Displayed only if global entitlements have been created and initiated for a pod federation in a Cloud Pod Architecture environment) Click **Not Set** and add an item from the **New value** drop-down menu.

6 To run the workflow, click **Submit**.

Results

The delegated administrator user or group that you selected can now manage the desktop and application pools that you specified in the form.

Configuration Tasks for Self-Service Workflows and Unmanaged Machines

To enable self-service features and management of virtual machines that have not yet been added to a pod, you must run certain configuration workflows.

1 Set access rights for delegated administrators on the **GuestCredentialConfiguration** and **SelfServicePoolConfiguration** configuration elements in the `View` folder. For information, see Best Practices for Managing Workflow Permissions.

2 In the `Configuration/Horizon Registration Configuration` folder, run the Add Guest Credential workflow before using any of the workflows for registering unmanaged machines.

   Unmanaged machines are virtual machines that a vCenter Server instance manages, but that have not been added to VMware Horizon. If you log in to Horizon Console and navigate to **View Configuration > Servers > vCenter Servers**, you cannot see the vCenter Server instance in the list.

You must register an unmanaged machine with a Connection Server instance before you can add the virtual machine to a manual desktop pool. To run the Add Guest Credential workflow, you must have local or domain administrator credentials for the virtual machine.

3 Run the Manage Delegated Administrator Configuration for Registration workflow in the `Configuration/Horizon Registration Configuration` folder.

   This workflow enables the specified delegated administrator to use the guest credentials and access the data center or virtual machine folder that contains the unmanaged virtual machine.

4 Run the appropriate Manage Self Service Pool Configuration workflow.

   This workflow specifies which desktop and application pools are available for self-service workflows in the `Workflows/vCAC` folder.

   For desktop and application pools that are provided through a pod or federation, the Manage Self Service Pool Configuration workflow is located in the `Configuration/Self Service Pool Configuration` folder.

Best Practices for Managing Workflow Permissions

You can use vRealize Orchestrator to limit the personas that can view and interact with the workflows. Ideally, only the administrator interacts with workflows in vRealize Orchestrator. Delegated administrators and end users interact with the workflows through vSphere Web Client or vRealize Automation.

vRealize Orchestrator Plug-in for Horizon installs several workflows that are organized into directories in the vRealize Orchestrator user interface. The `API access` and `Business logic` folders are not meant to be modified because their contents form the building blocks of the other executable workflows. To prevent unauthorized customization of workflows, for certain folders, remove edit permissions for all users except the administrator, as a best practice.

Note The suggested permission settings in this topic are required only if you want to hide the `CoreModules` folder and the configuration elements in the `View` folder from delegated administrators and end users.

In the **Workflows** view, you can set the following access rights:

- On the root folder in the left pane, set the access rights so that delegated administrators have only View and Execute permissions.
- On the `Configuration` folder and `CoreModules` folder, set the access rights so that delegated administrators have no permissions and cannot see the folders. This restriction overrides the permissions set at the root folder.
- On the `Business logic` folder in the `CoreModules` folder, set the access rights so that delegated administrators have only View permissions.
- On the `API access` folder in the `CoreModules` folder, set the access rights so that delegated administrators have only View permissions.

- On the `vSphereWebClient` folder, set the access rights so that delegated administrators have only View permissions.

If you are unfamiliar with the procedure for setting access rights, see "Set User Permissions on a Workflow" in the vRealize Orchestrator documentation.

In the **Configurations** view, you can set the following access rights:

- On the `View` folder, set the access rights so that delegated administrators have no permissions.
- On all configuration elements inside the `View` folder, set the access rights so that delegated administrators have only View permissions.

If you are unfamiliar with the procedure for setting access rights, see "Create a Configuration Element" in the vRealize Orchestrator documentation.

Set a Policy for De-Provisioning Desktop Virtual Machines

With the Add Pool Policy Configuration workflow, administrators can set safeguards for delegated administrators and end users regarding de-provisioning, or recycling, desktops. Administrators can select whether to delete the virtual machine, and can determine how to manage any associated persistent disks.

You must run this workflow once for each pool that has an active de-provisioning workflow. When de-provisioning the virtual machines in a desktop pool, you can delete the virtual machine, or you can unassign and unentitle the user.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Configure the connection to the pod.

Procedure

1. Log in to vRealize Orchestrator as an administrator.
2. Click the **Workflows** view in vRealize Orchestrator.
3. In the workflows hierarchical list, select **Library > Horizon > Configuration > Pool Policy Configuration** and navigate to the **Add Pool Policy Configuration** workflow.
4. Right-click the **Add Pool Policy Configuration** workflow and select **Start workflow**.
5. Enter values in the form that appears and click **Submit**.

   If you save any persistent disks, specify the datastore and the path to the folder that stores the persistent disk.

What to do next

If you must remove or update a pool policy, you can run the Remove Pool Policy Configuration workflow or the Update Pool Policy Configuration workflow.

Using vRealize Orchestrator Plug-in for Horizon Workflows 3

You can use the predefined workflows installed by vRealize Orchestrator Plug-in for Horizon, or you can copy and customize workflows.

Note For security reasons, you can run configuration workflows only from within vRealize Orchestrator.

The folders and workflows that appear in the `Horizon` folder are the predefined workflows that vRealize Orchestrator Plug-in for Horizon delivers. To customize a workflow, create a duplicate of that workflow. Duplicate workflows, or custom workflows that you create, are fully editable.

For information about the access rights that you can have when you work with the vRealize Orchestrator server, depending on the type of vCenter Server license, see the *Installing and Configuring VMware vRealize Orchestrator* document.

This chapter includes the following topics:

- Access the vRealize Orchestrator Plug-in for Horizon Workflow Library
- vRealize Orchestrator Plug-in for Horizon Workflow Library
- vRealize Orchestrator Plug-in for Horizon Workflow Reference
- Syntax for Specifying User Accounts in the Workflows

Access the vRealize Orchestrator Plug-in for Horizon Workflow Library

To access the elements from the vRealize Orchestrator Plug-in for Horizon workflow library, you must use the vRealize Orchestrator client or vSphere Web Client.

Prerequisites

- Configure the connection to the pod. See Configure the Connection to a Pod in VMware Horizon.
- Verify that you have credentials for logging in to vRealize Orchestrator as a user that can run vRealize Orchestrator Plug-in for Horizon workflows.

Procedure

1. Log in to vRealize Orchestrator.
2. Click the **Workflows** view in vRealize Orchestrator.
3. Expand the hierarchical list to **Library** > **Horizon** > **Workflows**.
4. Review the workflow library.

vRealize Orchestrator Plug-in for Horizon Workflow Library

The workflow library for vRealize Orchestrator Plug-in for Horizon contains workflows that you can use to run automated processes to manage pods, including objects such as remote desktops and published applications, pools, entitlements, and Connection Server configuration.

The folders and workflows that vRealize Orchestrator Plug-in for Horizon provides are created in the `Horizon` folder. These workflows are organized into subfolders, according to purpose and functionality. Modifying this folder structure does not affect workflow execution.

Caution Some folders contain workflows on which other workflows depend. Do not modify these workflows.

Table 3-1. Folders Included with the vRealize Orchestrator Plug-in for Horizon Plug-In

Folder Name	Description
`Horizon`	Root folder for vRealize Orchestrator Plug-in for Horizon.
`CoreModules/API Access`	API layer for the workflows. **Important** Do not modify the contents of this folder.
`CoreModules/Business Logic`	Business logic for workflow interactions between the execution layers and the API Access layer. **Important** Do not modify the contents of this folder.
`Configuration`	Workflows for setting up and administering other workflows. Only administrators can run Configuration workflows from within the vRealize Orchestrator client.
`Configuration/Workflow Delegation`	Workflows that an administrator can use to test whether a particular delegated administrator can successfully run the workflow. If the delegated administrator does not have the correct permission, some workflows might run in vSphere Web Client, but not show a permissions error.
`Workflows/Example`	Workflows that you can use as a basis for creating customized workflows. **Note** If you set the workflow permissions as mentioned in this document, only the primary administrator can run the Add Pool Policy in Batch workflow.

Table 3-1. Folders Included with the vRealize Orchestrator Plug-in for Horizon Plug-In (continued)

Folder Name	Description
`Workflows/vCAC`	Workflows that an administrator uses to create catalog items from within vRealize Automation. Some workflows in this folder are self-service workflows that end users can use for self-service access to remote desktops and published applications. These workflows are meant to be run only in vRealize Automation.
`Workflows/vSphereWebClient`	Workflows that administrators, or delegated administrators, can run in vSphere Web Client and in the vRealize Orchestrator client.

vRealize Orchestrator Plug-in for Horizon Workflow Reference

Each workflow has a specific purpose and requires certain inputs.

Add Managed Machines to Pool

This workflow enables a delegated administrator to add vCenter Server-managed machines to a manual desktop pool.

For a machine to be considered a managed machine, the vCenter Server instance that manages the machine must be added to VMware Horizon. For example, in Horizon Console, you can navigate to **Settings > Servers > vCenter Servers**, and find the vCenter Server instance in the list.

Inputs/parameters	Pod, pool ID, or list of virtual machines.
Results	The selected virtual machines in a manual desktop pool.

Add Unmanaged Machines to Pool

This workflow enables a delegated administrator to add unmanaged virtual machines to a manual desktop pool. A vCenter Server instance manages the unmanaged machines, but the vCenter Server instance is not added to VMware Horizon.

Note This workflow does not add physical machines or non-vSphere virtual machines. To add those types of machines, see Adding Physical Machines and Non-vSphere Virtual Machines to Pools.

Inputs/ parameters	Pod, pool ID, list of virtual machines, or guest credentials. For more information, see the Limitations row in this table.
Prerequisites	See Prerequisites for Adding Unmanaged Machines to Pools.

Results	The selected virtual machines are registered and added to a manual desktop pool. If you try to use this workflow to add multiple machines, but some machines are not added, the workflow fails. Error messages appear in the log file, specifying why the machines were not added. Other machines are added successfully.
Limitations	■ To add a machine back to an unmanaged pool that you previously removed from the pool in VMware Horizon, wait for some time before adding the machine back to the pool. ■ Select virtual machines only from vCenter Server instances that have not been added to VMware Horizon. All vCenter Server instances are listed, meaning that vCenter Server instances that have been added to VMware Horizon are not filtered out. ■ If all the virtual machines from the vCenter Server instance do not appear in the virtual machine folder, you can select machines from individual host folders. This issue can occur when you have many virtual machines. ■ After you run the Add Guest Credentials workflow and the Manage Delegated Administrator Configuration for Registration workflow, guest credentials might not be populated in the vRealize Automation service catalog for several minutes. You might have to log out of vRealize Automation, and log back in, to see the credentials. ■ If you remove guest credentials by running the Remove Guest Credential workflow, you must also run the Refresh Delegated Administrator Configuration workflow in the `Configuration/Delegated Admin Configuration` folder. If you do not do so, when you run the Add Unmanaged Machines to Pool workflow, you might see the previous guest credentials in the drop-down menu in the workflow. If you select these credentials and run the workflow, you receive the `Can not find credential named TestCredentials Dynamic Script Module name :getGuestCredential#7)` error message.

Add Users to an App Pool

This workflow enables a delegated administrator to entitle users to an application pool.

Inputs/parameters	Pod, pool ID, or user names.
Results	Entitled users get direct access to the specified application.

Add Users to App Pools

This workflow enables a delegated administrator to entitle users to multiple application pools.

Inputs/parameters	Pod, pool IDs, or user names.
Results	Entitled users get direct access to the specified applications.

Add Users to a Desktop Pool

This workflow enables a delegated administrator to entitle users to a desktop pool.

Inputs/parameters	Pod, pool ID, or user names.
Results	Users are entitled to the specified desktop pool. Users can get a machine for floating pools, or automatically assigned dedicated pools (subject to availability). For other types of pools, users must be assigned to the machine explicitly through the assignment workflows.

Advanced Desktop Allocation

This workflow enables a delegated administrator to allocate a machine to a user by specifying either **Horizon View** or **vRealize Automation** as the machine provider.

This workflow requires a set of configuration steps before using **vRealize Automation** as a provider. See Chapter 6 Creating Machines and Managing Pools in vRealize Automation, and especially the topic Configure a Machine Blueprint Service for Advanced Desktop Allocation.

Inputs/ parameters	Machine provider (**Horizon View** or **vRealize Automation**), pod, pool ID, user name, or vRealize Automation catalog item (if you select vRealize Automation as the machine provider).
Binding requirements	The administrator can bind the catalog item to a specific blueprint to avoid giving the delegated administrator access to all catalog items in vRealize Automation.
Results	If you select **Horizon View** as the machine provider, this workflow behaves the same way as the Desktop Allocation workflow. If you select **vRealize Automation** as the machine provider, the workflow supports only manual pools. The following tasks are performed, in the following order: 1 A machine is provisioned using vRealize Automation. 2 The machine is registered in a desktop pool. 3 For a floating desktop pool, the end user is entitled to the pool. 4 For a dedicated desktop pool, the end user is assigned to the machine and is entitled to the pool. 5 The machine is added to the user's vRealize Automation **Items** tab as a vCAC machine, on the **Machines** panel. For more information, see Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users.
Limitations	■ Horizon Agent must be installed and running in the template that is used in the machine blueprint to provision the machines. See Create Templates and Blueprints for Adding Machines to Desktop Pools. ■ Update VMware Tools to the latest version in the template that the machine blueprint uses to provision the machines. See Create Templates and Blueprints for Adding Machines to Desktop Pools. ■ For unmanaged machines, valid user credentials that have Administrator access for the guest operating system on the machine must be provided. ■ For unmanaged machines, a vSphere customization specification must be provided in the blueprint. This customization specification must include a configuration to change the host name and SID of the machine so that each machine that is created from the template has a unique host name and SID. See Create Templates and Blueprints for Adding Machines to Desktop Pools. ■ Guest credentials must be added by running the Add Guest Credentials workflow. ■ Delegated Admin permissions must be provided on credentials by running the Manage Delegated Administrator Configuration for Registration workflow in the `Horizon/Configuration/Horizon Registration Configuration` folder. ■ If the administrator does not bind a machine blueprint to the catalog item, the delegated administrator must select only those catalog items (blueprints) that the administrator specifies to provision machines. For information about binding catalog items, see Import the Advanced Desktop Allocation Workflow.

Application Entitlement

This workflow enables a delegated administrator to entitle users to an application pool and to remove users' entitlements.

Inputs/ parameters	Pod, pool ID, users to entitle, or users to unentitle, which are selected from a default list. **Note** If you accidentally supply a desktop pool ID rather than an application pool ID, the workflow runs and does not display an error message. This issue occurs regardless of whether you manually supply the pool ID or whether you bind the workflow to a desktop pool ID.
Results	You can add and remove entitlements in the same workflow.

Assign User

This workflow assigns a user to a specific machine in a desktop pool. This workflow also includes an option to entitle the user to a desktop pool.

Inputs/parameters	Pod, pool ID, machine name, or user name.
Limitations	User assignment is not supported for floating pools.
Results	The user is assigned to the specified machine. The existing assignment is removed and the existing session, if any, is logged off forcibly.

Desktop Allocation

This workflow entitles the user to the specified desktop pool and, for dedicated-assignment pools, assigns a machine to the user, depending on availability. A new machine is provisioned for the user if the pool type is "specified naming."

Inputs/ parameters	Pod, pool ID, or user name.
Results	■ For floating desktop pools and session-based pools from RDS hosts, the user is entitled to the pool. ■ For automatically assigned dedicated pools, the user is entitled to the pool and assigned to an available machine, if any. ■ For dedicated pools that do not use an automatic naming pattern, a virtual machine is provisioned for the user with the name that the administrator specifies.

Desktop Allocation for Users

This workflow entitles multiple users to desktops in floating-assignment pools or RDS desktop pools. For dedicated-assignment pools, this workflow entitles and assigns multiple users to machines, depending on availability.

If the pool type is "specified naming," new machines are provisioned for users.

Inputs/ parameters	Pod, pool ID, user names, or machine names for a specified naming pool.

Results	- For floating desktop pools and session-based pools from RDS hosts, the users are entitled to the pool. - For automatically assigned dedicated pools, users are entitled to the pool and assigned to an available machine, if any. - For dedicated pools that do not use an automatic naming pattern, virtual machines are provisioned for users with the names the administrator specifies.
Limitations	- Machines are provisioned line by line. If the workflow fails for one machine, the other machines are not provisioned. - If you select a specified naming pool, to add a new line in the text box for adding machine names so that you can add multiple names, press Ctrl+Enter. If you press only Enter, the workflow is submitted instead of adding a new line.

Desktop Assignment

This workflow enables a delegated administrator to assign a user to a specific virtual machine and, optionally, entitle the user to the machine. It also enables a delegated administrator to remove an assignment for a user from a specific virtual machine in the same workflow.

Inputs/parameters	Pod, pool ID, machine name, user to assign, or user to unassign.
Limitations	User assignment is not supported for floating pools.
Results	Desktop assignments can be added and removed in the same workflow.

Desktop Entitlement

This workflow enables a delegated administrator to entitle users to a desktop pool and remove user entitlements.

Inputs/parameters	Pod, pool ID, users to entitle, or users to unentitle, selected from a default list.
Results	Entitlements can be added and removed in the same workflow.

Desktop Recycle

This de-provisioning workflow removes user assignment or entitlement from the specified virtual machine desktop. Depending on the pool policy, the virtual machine might be deleted and any persistent disks might be saved.

Inputs/parameters	Pod, pool ID, or user name.
Scope	Works for all types of pools.
Prerequisites	Run the Add Pool Policy Configuration workflow before running this workflow.
Results	For floating pools, user entitlement is removed. For other desktop pool types, user assignment is removed. For dedicated linked-clone pools, the virtual machine is deleted and persistent disks are saved according to the settings used in the Add Pool Policy Configuration workflow.
Limitations	- Saving a persistent disk (sometimes called a UDD, or user data disk), works only for automated dedicated linked-clone desktop pools. - Deleting the virtual machine is not supported for floating pools or manual pools.

Duplicate a Desktop Pool

This workflow enables a delegated administrator to create identical desktop pools using an existing desktop pool.

Prerequisites	The administrator must enable the **Use View Storage Accelerator** check box when creating the desktop pool. For more information, see the *Setting Up Virtual Desktops in Horizon* document.
Inputs/parameters	Pod, pool ID, name for the new cloned pool, or naming pattern. **Note** The underscore '_' is not supported in pool naming pattern for Horizon 7 version 7.1 and later. However, this is supported in Horizon 7 version 7.0.3 and earlier versions.
Results	The source desktop pool is duplicated.

Global Entitlement Management

This workflow enables a delegated administrator to add and remove users from a global entitlement.

Prerequisites	The administrator must give the delegated administrator permissions on global entitlements by running the Add Delegated Administrator Configuration workflow, or the Update Delegated Administrator Configuration workflow.
Inputs/ parameters	Pod federation, global entitlement name, users names to add, or user names to remove. **Note** In the **View Pod Federation** list, if you have set a default pod, that pod might not be selected because this workflow applies to the pod federation rather than to a specific pod. You can select a pod from the list. If duplicate federation names exist, the pod names appear in parentheses.
Results	Specified users are added or removed from a global entitlement.

Port Pool to vCAC

This workflow enables a delegated administrator to import desktop pools into vRealize Automation. You can manage these pools directly from the vRealize Automation console.

This workflow requires a set of configuration steps before importing and managing the pools in vRealize Automation. See Chapter 6 Creating Machines and Managing Pools in vRealize Automation and Use Machine Blueprints to Create and Add Desktops to Pools.

Inputs/parameters	Pod or pool ID.
Results	The specified pool is imported into vRealize Automation, and pool items appear on the delegated administrator's **Items** tab.

Register Machines to Pool

This workflow registers the supplied machine DNS names with a manual pool of unmanaged desktops in VMware Horizon. Use this workflow only for physical machines and non-vSphere virtual machines.

As an alternative to running this workflow, you can use the Add Physical Machines to Pool workflow in the `Workflows/Example` folder. This workflow combines the actions of the Register Machines to Pool workflow and the PowerShell workflows mentioned in Run Workflows to Add Physical Machines as PowerShell Hosts.

Before you run the Add Physical Machines to Pool workflow, you must perform the tasks described in Configure a Physical Machine for an Unmanaged Pool and Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines. You must also satisfy the prerequisites listed in Prerequisites for Adding Unmanaged Machines to Pools

Inputs/ parameters	Pod, pool ID, machine DNS names, or guest OS.
Results	Provided machine names are registered with the specified unmanaged desktop pool in VMware Horizon.
Limitations	■ This workflow registers the DNS names that are provided without performing validation. The administrator must manually push the returned registry token to the registered machine. ■ To add a new line in the DNS Names text box so that you can add multiple DNS names, press Ctrl +Enter. If you press only Enter, the workflow is submitted instead of adding a new line.

Remove Users From Application Pool

This workflow removes multiple user entitlements from an application pool.

Inputs/parameters	Pod, pool ID, or users, selected from a default list.
Results	Specified users are no longer entitled to the specified application pool.

Remove Users From Desktop Pool

This workflow removes multiple user entitlements from a desktop pool.

Inputs/parameters	Pod, pool ID, or users, selected from a default list.
Results	Specified users are no longer entitled to the specified desktop pool.

Self-Service Advanced Desktop Allocation

This workflow enables end users to allocate machines to themselves, selecting either **Horizon View** or **vRealize Automation** as the machine provider.

This workflow requires a set of configuration steps before using **vRealize Automation** as a provider. See Chapter 6 Creating Machines and Managing Pools in vRealize Automationand Configure a Machine Blueprint Service for Advanced Desktop Allocation.

Inputs/ parameters	Machine provider (**Horizon View** or **vRealize Automation**), pod, pool ID, or vRealize Automation catalog item, if you select vRealize Automation as the machine provider.
Binding requirements	The administrator can bind the catalog item to a specific blueprint to avoid giving the end user access to all catalog items in vRealize Automation.

Results

If you select **Horizon View** as the machine provider, this workflow behaves the same way as the Self-Service Desktop Allocation workflow.

If you select **vRealize Automation** as the machine provider, the workflow supports only manual pools. The following tasks are performed, in the following order:

1. A machine is provisioned using vRealize Automation.
2. The machine is registered in a desktop pool.
3. For a floating-assignment desktop pool, the end user is entitled to the pool.
4. For a dedicated-assignment desktop pool, the end user is assigned to the machine and entitled to the pool.
5. The machine is added to user's vRealize Automation **Items** tab as a vCAC machine, on the **Machines** panel.
6. The machine is added to the user's vRealize Automation **Items** tab as a desktop, on the **Horizon** panel.
7. If the machine was already added to the **Items** tab, on the **Machines** panel, and the user runs the workflow again but selects **Horizon View** as the provider, the machine is also added to the **Items** tab on the **Horizon** panel.

For more information, see Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users.

Limitations

- Horizon Agent must be installed and running in the template that the machine blueprint to provision the machines uses. See Create Templates and Blueprints for Adding Machines to Desktop Pools.
- VMware Tools must be updated to latest version in the template that the machine blueprint to provision the machines uses. See Create Templates and Blueprints for Adding Machines to Desktop Pools.
- For unmanaged machines, you must provide valid user credentials that have Administrator access for the guest operating system on the machine.
- For unmanaged machines, you must provide a vSphere customization specification in the blueprint. This customization specification must include a configuration to change the host name and SID of the machine so that each machine created from the template has a unique host name and SID. See Create Templates and Blueprints for Adding Machines to Desktop Pools.
- You must add guest credentials by running the Add Guest Credentials workflow.
- The administrator must provide end users with the permission to use guest credentials by running the Manage Self-Service Configuration for Registration workflow in the `Horizon/Configuration/Horizon Registration Configuration` folder.
- If the administrator does not bind a machine blueprint to the catalog item, the end user must select only those catalog items (blueprints) that the administrator specified to provision machines. For information about binding catalog items, see Import the Self-Service Advanced Desktop Allocation Workflow.

Self-Service Desktop Allocation

This workflow enables end users to allocate a machine to themselves. A new machine is provisioned only for "specified naming" desktop pools.

Inputs/parameters	None.
Scope	Works only on automated pools.

Prerequisites/ binding requirements	The administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. This workflow does not appear in the `vSphereWebClient` folder.
Results	■ For floating desktop pools and session-based pools from RDS hosts, the user is entitled to the pool. ■ For automatically assigned dedicated pools, the user is entitled to the pool and assigned to an available machine (if any). ■ For dedicated pools that do not use an automatic naming pattern, a virtual machine that has the specified name is provisioned for the user.

Self-Service Desktop Recycle

This workflow enables end users to de-provision their own virtual machines from a specified pod and desktop pool. This workflow removes user entitlements and assignments. Depending on the pool policy, the virtual machine might be deleted and any persistent disks might be saved.

Inputs/parameters	None.
Limitations	■ Saving a persistent disk, sometimes called a use data disk (UDD), works only for automated dedicated linked-clone desktop pools. ■ Deleting the virtual machine is not supported for floating pools or manual pools.
Prerequisites/ binding requirements	To specify which pools are available for selection by end users, the administrator must run the Manage Self Service Pool Configuration workflow. This workflow does not appear in the `vSphereWebClient` folder.
Results	For floating-assignment pools, user entitlements are removed. For other desktop pool types, user assignments are removed. For dedicated-assignment linked-clone pools, the virtual machine is deleted and persistent disks are saved according to the settings used in the Add Pool Policy Configuration workflow.

Self-Service Release Application

This workflow enables end users to remove their entitlement from the specified application pool.

Inputs/parameters	None.
Prerequisites/binding requirements	The administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. This workflow does not appear in the `vSphereWebClient` folder.

Self-Service Request Application

This workflow enables end users to request an application for their own use. Users are entitled to the specified application pool.

Inputs/parameters	None.
Prerequisites/binding requirements	The administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. This workflow does not appear in the `vSphereWebClient` folder.

Self Service Request Application Stack

This workflow enables end users to request an application stack for their own use. Users are entitled to the specified application stack after receiving approval from the appropriate owner.

Inputs/parameters	Specify an application stack from a drop-down menu.
Prerequisites	The administrator must run the Add an App Volumes Server workflow.
Results	The end user is entitled to use the requested application stack after an administrator has approved the request.
Limitations	None.

Session Management

This workflow enables delegated administrators to disconnect, log out, reset, and send messages to active remote desktop sessions. Delegated administrators can perform these operations on user sessions.

Inputs/ parameters	Pod, pool ID, operation, message (for the Send Message operation), user name, and other options.
Results	The selected operation is performed on the specified session.
Limitations	■ Application sessions are not supported. ■ The reset operation is not supported for RDS pools, manual unmanaged desktop pools, and instant clone pools. ■ Selection of multiple sessions is not supported when this workflow runs from vSphere Web Client or the vRealize Orchestrator client. ■ The predefined list of users does not appear when this workflow runs from vRealize Automation.

Set Maintenance Mode

This workflow enables a delegated administrator to add and remove machines from maintenance mode.

Inputs/parameters	Pod, pool ID, operation, or virtual machine.
Binding requirements	For the `vSphereWebClient` folder, the administrator must bind the workflow to a pod while using vRealize Orchestrator and add it to the delegated admin group.
Results	The selected machines are "entered into maintenance mode" or "exited from maintenance mode".
Limitations	This workflow is not supported for RDS pools, manual unmanaged desktop pools, and instant clone pools.

Unassign User

This workflow removes the assignment of a user from a virtual machine.

Inputs/parameters	Pod, pool ID, or machine name as shown in Horizon Console.
Limitations	User assignment is not supported for floating pools.
Results	The user's assignment is removed and entitlement to the pool remains unchanged. The user's session is logged off forcibly.

Update App Pool Display Name

This workflow changes the display name of an application pool.

Inputs/parameters	Pod, pool ID, or a new display name for the pool.
Results	The display name changes, but the pool ID remains the same.

Update Desktop Pool Display Name

This workflow changes the display name of a desktop pool.

Inputs/parameters	Pod, pool ID, or a new display name for the pool.
Results	The display name changes, but the pool ID remains the same.

Update Desktop Pool Min Size

Changes the minimum number of desktops that the pool can contain.

Scope	Works only for automated floating and automated dedicated pools that use a naming pattern.
Inputs/parameters	Pod, pool ID, or the number to use for the minimum pool size, which must be an integer.
Results	The minimum number of virtual machines in the pool changes. **Note** Consider whether your company's hardware resources are sufficient before increasing this number.

Update Desktop Pool Spare Size

This workflow changes the number of spare machines in the pool that are available and powered on for new users.

Scope	Works only for automated pools.
Inputs/parameters	Pod, pool ID, or the number of spare machines to have ready, which is an integer.
Results	Changes the number of spare virtual machines to keep ready and powered on for new users. **Note** Consider whether your company's hardware resources are sufficient before increasing this number.

Syntax for Specifying User Accounts in the Workflows

The syntax that you use for specifying users in the vRealize Orchestrator Plug-in for Horizon workflows is consistent across all workflows.

When supplying a user name, you must specify the user and domain by using one of the following formats:

- username@domain.com
- username@domain
- domain.com\username

- domain\username

If you have users in multiple domains, you might have users or groups with the same name but different domains. When using the search feature, you might see a list of users that have the same name. The list returns only the user name, and not the domain name. To see the complete domain name for a user or group, point your mouse at the name. A tooltip appears that shows the complete domain name.

Note Non-ASCII characters are not supported.

Making the Workflows Available in vSphere Web Client and vRealize Automation

4

Administrators can expose the VMware Horizon workflows in the vRealize Automation self-service catalog or in vSphere Web Client. For some workflows that delegated administrators run within vSphere Web Client, you must specify the pod or pools on which the workflows act.

This chapter includes the following topics:

- Exposing VMware vRealize Orchestrator Plug-in for Horizon Workflows in vSphere Web Client
- Exposing vRealize Orchestrator Plug-in for Horizon Workflows in vRealize Automation

Exposing VMware vRealize Orchestrator Plug-in for Horizon Workflows in vSphere Web Client

Administrators can configure VMware Horizon workflows so that delegated administrators can run the workflows from within vSphere Web Client. The delegated administrator can search for the name of the workflow and run and schedule vRealize Orchestrator workflows.

Bind vSphere Web Client Workflows to Specific Pods and Pools in vRealize Orchestrator

When a delegated administrator's access must be restricted to particular pools or pods, you can bind a workflow to a specific pool or pod. Administrators can duplicate workflows and bind the workflows to different pools as needed.

After an administrator binds a workflow to a pod, the delegated administrator sees a drop-down menu of the pools that belong to that pod in vSphere Web Client. You can also bind the workflow to a specific pool and disable the drop-down menu of pools. Drop-down menus of pools are supported for most workflows, regardless of whether the workflows are localized.

For the following workflows, if you plan to localize the workflow, you must bind the workflow to a specific pool and disable the drop-down menu of pools:

- Application Entitlement
- Assign User
- Desktop Assignment

- Desktop Entitlement
- Unassign User

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the pod by running the Add View Pod in the Configuration workflow. See Configure the Connection to a Pod in VMware Horizon.
- Verify that you have assigned the correct delegated administrators to the pools that you plan to expose through vSphere Web Client. See Assign Delegated Administrators to Pools.

Procedure

1. Log in to the vRealize Orchestrator client as an administrator and select **Design** from the drop-down menu in the upper-left portion of the screen.
2. In the workflows hierarchical list, select **Library > Horizon** and navigate to the subfolder and workflow.

   For example, you might navigate to the Add Users to Desktop Pool workflow in **Library > Horizon > Workflows > vSphereWebClient**.
3. Right-click the workflow, select **Duplicate Workflow**, and enter values in the form.

   The new workflow appears in the folder that you selected.
4. Select the newly created workflow in the left pane, click the **Presentation** tab in the right pane, and click the **Edit** (pencil) icon in the toolbar at the top of the pane.
5. Select **(string)podAlias *Horizon View Pod*** in the upper portion of the tab and edit its properties.

   a. In the lower portion of the tab, click the **Properties** tab, and in the **Data Binding** row, type the pod name and enclose it with quotation marks, for example, `"ViewPod1"`.

   b. Select and delete the **Predefined answers** property.

   c. Add the **Default value** property and enter the same pod name enclosed in quotation marks.

   If you do not delete the **Predefined answers** property and set the **Default value** property, you might see a drop-down menu of pods in vSphere Web Client, even though the workflow is bound to one pod.

6 To bind the workflow to only one pool, select **(string)poolId *Desktop Pool ID*** in the upper portion of the tab and edit its properties.

   a In the lower portion of the tab, click the **Properties** tab, and in the **Data Binding** row, enter the pool ID and enclose it in quotation marks, for example, `"DesktopPool"`.

   b Select and delete the **Predefined answers** property.

   c Add the **Default value** property and type in the same pool name enclosed in quotation marks.

   If you do not delete the **Predefined answers** property and set the **Default value** property, you might see a drop-down menu of pods in vSphere Web Client, even though the workflow is bound to one pool.

Results

When this workflow starts, the pod name and pool ID are already populated and cannot be changed.

What to do next

Create versions of the workflow in other languages.

Create Localized Versions of a Workflow for vSphere Web Client

To create the localization resources for vSphere Web Client, administrators can run the Clone Localization Resources workflow in the `Configuration` folder.

Prerequisites

- Bind the workflow to a pod and, optionally, to a pool. See Bind vSphere Web Client Workflows to Specific Pods and Pools in vRealize Orchestrator.
- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.

Procedure

1 Log in to the vRealize Orchestrator client as an administrator and select **Design** from the drop-down menu in the upper-left portion of the screen.

2 Click the **Resources** view and navigate to the folder that contains the duplicated workflow that you used to bind the workflow to a pod.

3 In that folder, create a subfolder, and, for the folder name, specify the same name used for the duplicated workflow.

   The folder name must match the duplicated workflow name and must be in the same folder as the workflow.

4 Click the **Workflows** view and navigate to **Library > Horizon > Configuration**.

5 Expand the **Configuration** item, right-click the **Clone localization resources** workflow, and select **Start workflow**.

6 Enter values in the form as described in the following table.

Option	Action
Source Workflow	Click **Not Set** and select the original workflow that you duplicated to bind the workflow to a pod.
Target Workflow	Click **Not Set** and select the workflow that you duplicated.

7 To run the workflow, click **Submit**.

Results

If the workflow finishes successfully, you can select **Resources** view, expand the folder that you created, and see the properties files for each language.

Exposing vRealize Orchestrator Plug-in for Horizon Workflows in vRealize Automation

vRealize Automation provides a service catalog that contains a request and approval engine that enables fine-grained control of workflows through entitlement and auditing.

Administrators can add service and machine blueprints by browsing through **Orchestrator > Library > Horizon** and selecting a specific workflow. You can use standard vRealize Automation procedures to publish and entitle through Catalog Management. Because entitlement is usually specific when vRealize Automation uses the workflow, you must bind the workflow to a particular pod, desktop pool, or application pool.

Procedure

1 Create Business Groups for Delegated Administrators and End Users

In vRealize Automation, users must belong to a business group before they can be entitled to a service created for a VMware Horizon plug-in workflow.

2 Create Services for Delegated Administrators and End Users

In vRealize Automation, administrators must create a service to entitle users to catalog items.

3 Create Entitlements for Delegated Administrators and End Users

To create an entitlement in vRealize Automation, administrators specify a business group and the service that corresponds to that group.

4 Bind vCAC Workflows to a vCAC User

vCAC User is one of the required parameters for the workflows in the vCAC folder. You must configure that parameter to be requested by a principal ID.

5 Configure Output Parameters for vCAC Workflows

For workflows that return output parameters, you can add the output parameters to the service blueprint. An example of an output parameter is the URL for accessing the desktop through HTML Access.

6 Configure the Catalog Item for the Workflow

In vRealize Automation, administrators can configure workflows to appear in the catalog for delegated administrators and end users.

Create Business Groups for Delegated Administrators and End Users

In vRealize Automation, users must belong to a business group before they can be entitled to a service created for a VMware Horizon plug-in workflow.

If you have been using vRealize Automation, you might have already created these business groups, or equivalent business groups.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Become familiar with the procedures for creating groups in vRealize Automation. For information, see the vRealize Automation documentation.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Click the **Infrastructure** tab.

3 Create a fabric group that has the administrator as a member.

  a Select **Infrastructure > Endpoints > Fabric Group**.

  b Create a fabric group that has the administrator as a member.

4 Create a business group for the delegated administrators.

  a Select **Administration > User & Group > Business Group**.

  b Create a business group for the delegated administrators.

Option	Action
Group manager role	Use the administrator account that you added in the fabric group.
Users role	Add the delegated administrator users.

5 To add the new group, click **OK**.

6 Click **Business Groups** and create a business group for end users.

Option	Action
Group manager role	Use the administrator account that you added in the fabric group.
Users role	Add the end users.

7 To add the new group, click **OK**.

What to do next

Create corresponding services for delegated administrators and end users.

Create Services for Delegated Administrators and End Users

In vRealize Automation, administrators must create a service to entitle users to catalog items.

If you have been using vRealize Automation, you might have already created these services, or equivalent services.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Become familiar with the procedures for creating services in vRealize Automation. For information, see the vRealize Automation documentation.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Click the **Administration** tab.

3 Select **Catalog Management > Services**.

4 Create a service for the delegated administrators business group.

   a Click the **Add Service** (+) icon.

   b On the **Details** tab, supply a name, and in the **Status** list, select **Active**.

   c Click **Add**.

5 To create a service for the end users business group, repeat previous step .

What to do next

Create entitlements for delegated administrators and end users.

Create Entitlements for Delegated Administrators and End Users

To create an entitlement in vRealize Automation, administrators specify a business group and the service that corresponds to that group.

If you have been using vRealize Automation, you might have already created these entitlements, or equivalent entitlements.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Create the business groups that contain the users that you want to entitle. See Create Business Groups for Delegated Administrators and End Users.
- Create the services that correspond to the business groups that you want to entitle. See Create Services for Delegated Administrators and End Users.
- Become familiar with the procedures for creating entitlements in vRealize Automation. For information, see the vRealize Automation documentation.

Procedure

1. Log in to vRealize Automation as an administrator.
2. Click the **Administration** tab.
3. Select **Catalog Management > Entitlements**.
4. Create an entitlement for delegated administrators.
   a. Click the **Add Entitlement** (+) icon.
   b. On the **Details** tab, enter a name and, in the **Status** list, select **Active**.
   c. From the **Business Group** list, select the business group that you created for delegated administrators.
   d. In the **Users & Groups** text box, specify users from the delegated administrators business group and click **Next**.
   e. On the **Items & Approvals** tab, click the **Add** (+) icon for **Entitled Services** and select the delegated administrator service that you created.
   f. Click **Add**.
5. To create an entitlement for end users, repeat the previous step.

What to do next

Bind the vRealize Orchestrator Plug-in for Horizon workflows to pods and pools.

Bind vCAC Workflows to a vCAC User

vCAC User is one of the required parameters for the workflows in the vCAC folder. You must configure that parameter to be requested by a principal ID.

You can customize workflows that are exposed through vRealize Automation by using the vRealize Automation form editor interface. You can hide or rearrange fields and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize it as needed. You can convert any workflow field to a text box, or provide values to display so that users can select values from a drop-down menu.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the pod by running the Add View Pod in Configuration workflow. See Configure the Connection to a Pod in VMware Horizon.
- Verify that vRealize Automation is configured to communicate with the vRealize Orchestrator server so that the vRealize Orchestrator workflows are available.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Add a new Service Blueprint.

  a Select **Design > XaaS > XaaS Blueprints**.

  b Click **New** (+) icon.

3 Navigate through the vRealize Orchestrator workflow library and select a workflow from the **Library > Horizon > Workflows > vCAC** folder.

4 Click **Next** and enter the workflow name and description that will appear in the vRealize Automation service catalog.

5 Click **Next** and, on the **Blueprint Form** tab, edit the **vCACUser** text box.

  a Click in the **vCACUser** text box and click the **Edit** (pencil) icon.

  b In the Edit Form Field - vCACUser dialog box, click the **Constraints** tab.

  c Click to expand the **Value:** drop-down list.

  d Select the **Field** radio button and click to expand the **Request Info** item.

  e Click to expand the **Requested by** item and select **Principal ID**.

  f Click to expand the **Visible:** drop-down list.

  g Select the **Constant** radio button and select **No** to hide this parameter in the catalog request.

  h Click **Submit**.

6 On the **Provisioned Resource** tab, click **Add**.

  The blueprint appears on the Service Blueprints page and the status is set to Draft.

7 To publish the blueprint, select **Publish** from the **Actions** list for the blueprint.

Results

The item appears on the **Administrator > Catalog Management > Catalog Items** tab.

What to do next

Configure the catalog item for this service.

Configure Output Parameters for vCAC Workflows

For workflows that return output parameters, you can add the output parameters to the service blueprint. An example of an output parameter is the URL for accessing the desktop through HTML Access.

You can customize workflows that are exposed through vRealize Automation by using the vRealize Automation form editor interface. You can hide or rearrange fields and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize it as needed. You can convert any workflow field to a text box, or provide values to display so that users can select from a drop-down menu.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the pod by running the Add View Pod in Configuration workflow. See Configure the Connection to a Pod in VMware Horizon.
- Verify that vRealize Automation is configured to communicate with the vRealize Orchestrator server so that the vRealize Orchestrator workflows are available.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Add a new service blueprint.

   a Select **Design > XaaS > XaaS Blueprints**.

   b Click **New** (+) icon.

3 Navigate through the vRealize Orchestrator workflow library and select a workflow from the **Library > Horizon > Workflows > vCAC** folder.

4 Click **Next** and enter the workflow name and description that appears in the vRealize Automation service catalog.

5 Click **Next** and, on the **Blueprint Form** tab, click the plus icon (**+**).

6 In the New Form dialog box, title the form **Request Details**, and in the **Screen type** list, select **Submitted request details**, and click **Submit**.

   In the Fields list on the left side of the form, you can scroll down and see a new section called **Outputs**.

7 Click a parameter item under **Outputs** in the Fields list and drag it onto the form page.

   For example, if you were creating a blueprint from a desktop allocation workflow, you can click the **htmlAccessUrl** item under **Outputs** in the Fields list and drag the **htmlAccessUrl** item onto the form page.

8 Click **Next** and, on the **Provisioned Resource** tab, click **Add**.

   The blueprint appears on the Service Blueprints page and the status is set to Draft.

9 To publish the blueprint, select **Publish** from the **Actions** list for the blueprint.

Results

The item now appears on the **Administrator > Catalog Management > Catalog Items** tab.

What to do next

Configure the catalog item for this service. After a user submits a request by using this catalog item, if you select the **Requests** tab and view the details of one of the requests for this item, the output parameters appear on the **Step** tab.

Configure the Catalog Item for the Workflow

In vRealize Automation, administrators can configure workflows to appear in the catalog for delegated administrators and end users.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have published the workflow as a service blueprint. See Bind vCAC Workflows to a vCAC User.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Select **Administration > Catalog Management > Catalog Items**.

3 Click the item name in the list.

4 On **Configure Catalog Item** tab, from the **Service** list, select the service for the delegated administrator or end user and click **Update**.

Results

The workflow is now ready for the delegated administrator or end user to run. When the delegated administrator or end user logs in to vRealize Automation and selects the **Catalog** tab, the service or workflow appears. To run the workflow, the user clicks the **Request** button, enters values in the form that appears and clicks **Submit**.

To check the status of the request, the user selects the **Request** tab.

The primary administrator can check the status by logging in to vRealize Orchestrator, clicking the expander button next to the workflow, and selecting the workflow to run.

Making Desktop and Pool Actions Available in vRealize Automation 5

Administrators can create desktop machine and pool items and make them available on the **Items** tab of vRealize Automation. Administrators can also create a list of actions that end users and delegated administrators can perform on machines and pools. For example, end users can start, reboot, and recycle machines, and perform other actions. Delegated administrators can perform actions such as managing user entitlements, recomposing the pool, and other actions.

After you make items available, action items become available on the **Items** tab of vRealize Automation when you click **Horizon** in the left pane.

This chapter includes the following topics:

- Export Action Item Icons from vRealize Orchestrator
- Import Desktops and Pools as Custom Resources
- Import Actions for Desktop and Pool Items
- Import Workflows for Desktop and Pool Management
- Entitle Users to Action Items
- Import Action Icons into vRealize Automation

Export Action Item Icons from vRealize Orchestrator

Although you can configure action items to appear in desktop and pool details in vRealize Automation without using the icons supplied by vRealize Orchestrator, as a best practice, export the icons from vRealize Orchestrator and import them into vRealize Automation.

To find a listing of the available actions, go to the **Workflows** view in vRealize Orchestrator and navigate to **Library > Horizon > Workflows > vCAC > Actions**. The actions appear in the `Desktop` and `Pool` folders.

Prerequisites

Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.

Procedure

1. Log in to vRealize Orchestrator as an administrator and select **Design** from the drop-down menu in the upper-left portion of the screen.
2. Click the **Resources** view in vRealize Orchestrator.
3. Navigate to **Library > Horizon > Icon**.
4. To save the icon file to your local system, right-click an icon file and select **Save to file**.
5. Repeat this step for all the actions that you plan to make available on the **Items** tab in vRealize Automation.

What to do next

Import the custom resources that you need for these actions. See Import Desktops and Pools as Custom Resources.

Import Desktops and Pools as Custom Resources

The first stage of configuring action items in vRealize Automation is to create `ViewDesktop` and `ViewPool` custom resources. You can then select these resources when you import actions and workflows, such as the Self-Service Advanced Desktop Allocation workflow.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that vRealize Automation is configured to communicate with the vRealize Orchestrator server so that the vRealize Orchestrator workflows are available.

Procedure

1. Log in to vRealize Automation as an administrator.
2. To create a Custom Resource, select **Design > XaaS > Custom Resources**.
3. Click the **Add** (+) icon.
4. On the **Resource type** tab, enter **`horizon`** in the **Orchestrator Type** text box.

   A list of items matching those letters appears.
5. Select **Horizon: HorizonViewDesktop**.
6. For the name, enter **`ViewDesktop`** and click **Next**.
7. On the **Details Form** tab, click **Finish**.

   You do not need to make any changes on this page.

8 Repeat the procedure for pools.

   a On the **Resource type** tab, in the **Orchestrator Type** text box, enter `horizon`.

   b Select **Horizon: HorizonViewPool**.

   c For the name, enter `ViewPool` and click **Next**.

   d On the **Details Form** tab, delete the **Available Actions** field and click **Finish**.

   Deleting the **Available Actions** field prevents extraneous text from being shown on the **Details** tab when the delegated administrator later clicks the pool item on the **Items** tab.

Results

The new resources appear on the **XaaS > Custom Resources** page.

What to do next

Import action items. See Import Actions for Desktop and Pool Items.

Import Actions for Desktop and Pool Items

After you define desktops and pools as resource types, you can assign actions to the desktops and pools.

Prerequisites

- Create the business groups that contain the users that use these actions. See Create Business Groups for Delegated Administrators and End Users.
- Verify that vRealize Automation is configured to communicate with the vRealize Orchestrator server so that the vRealize Orchestrator workflows are available.
- Import the required resource types. See Import Desktops and Pools as Custom Resources.

Procedure

1 Log in to vRealize Automation as an administrator.

2 To create a Resource Action, select **Design > XaaS > Resource Actions**.

3 Click the **Add** (+) icon.

4 On the **New Resource Action - Workflow** tab, navigate to **Library > Horizon > Workflows > vCAC > Actions**.

5 Expand the **Desktop** folder, select an action, and click **Next**.

6 On the **Input Resource** tab, click **Next**.

   The **Resource type** drop-down menu shows the **ViewDesktop** type that you imported.

7 On the **Details** tab, select the **Hide catalog request information page** check box.

   You can also change the name of the action. For example, instead of **Logoff**, you might use **Log off desktop**.

8 If you are importing the Recycle action or the Drop Pool action, on the **Details** tab, in the **Type** section, select the **Disposal** check box.

9 On the **Details** tab, in the **Target criteria** section, for the Drop Pool action only, select **Always available**and, for all other actions, select the **Available based on conditions** radio button, and use the following settings in the drop-down menus that appear.

List	Select
Clause	**Available Actions**
Operator	**Contains**
Value	**Constant**, and enter the appropriate value: `logoff`, `reboot`, `refresh`, `shutdown`, `start`, `drop-pool`, `manage-entitlement`, `manage-session`, `recompose`, `manage-assignment`, `recycle` or `duplicate-pool` .

The value must be in lowercase letters.

10 Click **Next**.

11 On the **Form** tab, if you are importing a desktop action, click **Finish**, or, if you are importing a pool action, edit the **vCACUser** text box to bind the action to a user.

a Click in the **vCACUser** text box and click the **Edit** (pencil) icon.

b In the Edit Form Field - vCACUser dialog box, click the **Constraints** tab.

c Click to expand the **Value:** drop-down menu.

d Select the **Field** radio button and click to expand the **Request Info** item.

e Click to expand the **Requested by** item and select **Principal ID**.

f Click to expand the **Visible:** drop-down menu.

g Select the **Constant** radio button and select **No** to hide this parameter in catalog request.

h Click **Submit**.

i On the **Form** tab, click **Add**.

12 To add other actions, repeat this process.

The action items appear on the **Resource Actions** page and the Status column shows that the items are in draft form.

13 On the **Resource Actions** page, select the action items one by one and click the **Publish** button above the table.

What to do next

Import the workflows that use these actions. See Import Workflows for Desktop and Pool Management.

Import Workflows for Desktop and Pool Management

You must create service blueprints that correspond to the workflows you plan to use for desktop and pool management.

This procedure involves importing the following workflows for end users:

- Self-Service Desktop Allocation
- Self-Service Advanced Desktop Allocation

You must import these workflows so that items for the workflows can appear on the end user's **Catalog** tab in vRealize Automation. After the end user submits a request to run the workflow, an item for the user's remote desktop appears on the user's **Items** tab in vRealize Automation.

When the user clicks the remote desktop item and goes to the **Item Details** tab, the user can access the configured actions for the remote desktop. The actions can include start, log out, reboot, shut down, and recycle. For linked-clone desktops, users can also use a refresh action to revert the machine back to the state it was in when the user first acquired the machine. In this way, end users can access and manage their machines from the vRealize Automation user interface.

This procedure also involves importing the following workflows for delegated administrators:

- Advanced Desktop Allocation

  After you import this workflow, an item for this workflow appears on the delegated administrator's **Catalog** tab in vRealize Automation. After the delegated administrator submits a request to run this workflow, the workflow performs one or more tasks to ensure that a machine is created and provisioned and is assigned to a user. Also, if necessary, the workflow creates an entitlement for the user. The result is that the end user has an item on the user's **Items** tab in vRealize Automation, and the end user can see the configured action buttons described for the self-service workflows.

- Port Pool to vCAC

  After you import this workflow, an item for this workflow appears on the delegated administrator's **Catalog** tab in vRealize Automation. After the delegated administrator submits a request to run this workflow, the workflow creates items for the specified pools, and these pool items appear on the delegated administrator's **Items** tab in vRealize Automation.

  When the delegated administrator clicks a pool item and goes to the **Item Details** tab, the delegated administrator can access the configured actions for desktop pool management. The actions can include drop pool (delete the pool), manage assignment, manage entitlement, manage session, and, for linked-clone pools, recompose. The result is that a delegated administrator can manage desktop pools using actions buttons in vRealize Automation.

Prerequisites

- Create the business groups that contain the users that use these actions. See Create Business Groups for Delegated Administrators and End Users.

- Verify that vRealize Automation is configured to communicate with the vRealize Orchestrator server so that the vRealize Orchestrator workflows are available.
- Import the actions for desktops and pools. See Import Actions for Desktop and Pool Items.

Procedure

1 Import the Self-Service Desktop Allocation Workflow

This workflow enables end users to allocate a machine to themselves.

2 Import the Self-Service Advanced Desktop Allocation Workflow

This workflow enables end users to allocate machines to themselves by selecting either **Horizon View** or **vRealize Automation** as the machine provider.

3 Import the Advanced Desktop Allocation Workflow

This workflow enables a delegated administrator to allocate machines to an end user, selecting either **Horizon View** or **vRealize Automation** as the machine provider.

4 Import the Assign an AppStack to User Workflow

This workflow enables end users to request an application stack for their own use.

5 Import the Self-Service Remote Application Workflow

This workflow enables end users to request a remote application for their own use.

6 Import the Port Pool to vCAC Workflow

This workflow enables a delegated administrator to import desktop pools into vRealize Automation and manage the pools directly from the vRealize Automation console.

Import the Self-Service Desktop Allocation Workflow

This workflow enables end users to allocate a machine to themselves.

Procedure

1 Log in to vRealize Automation as an administrator.

2 To select a new Service Blueprint, select **Design > XaaS > XaaS Blueprints**.

3 Click the **Add** (+) icon.

4 On the **Add Blueprint - Workflow** tab, navigate to **Library > Horizon > Workflows > vCAC**, select the workflow, and click **Next**.

5 On the **Details** tab, select the **Hide catalog request information page** check box and click **Next**.

6 On the **Blueprint Form** tab, click **Next**.

7 On the **Provisioned Resource** tab, select **desktop[ViewDesktop]** and click **Add**.

The blueprint appears on the **Service Blueprints** page and the Status column shows that the blueprint is in draft form.

8 On the **Service Blueprints** page, select the blueprint and click the **Publish** button above the table.

Results

The service blueprint for the workflow is published and appears in the **Advanced Services > Service Blueprints** table.

What to do next

Import other desktop allocation workflows.

Import the Self-Service Advanced Desktop Allocation Workflow

This workflow enables end users to allocate machines to themselves by selecting either **Horizon View** or **vRealize Automation** as the machine provider.

Procedure

1 Log in to vRealize Automation as an administrator.

2 To select a new Service Blueprint, select **Design > XaaS > XaaS Blueprints**.

3 Click the **Add** (+) icon.

4 On the **Add Blueprint - Workflow** tab, navigate to **Library > Horizon > Workflows > vCAC**, select the workflow, and click **Next**.

5 On the **Details** tab, select the **Hide catalog request information page** check box and click **Next**.

6 (Optional) On the **Blueprint Form** tab, bind the **Create Machine Catalog Item** field to a specific machine blueprint.

   Performing this task means that the end user or delegated administrator cannot navigate through the catalog of blueprints to select a blueprint. As a security measure, you can configure the workflow so that the blueprint is already selected.

   a On the **Blueprint Form** tab, click in the **Create Machine Catalog Item** text box and click the **Edit** (pencil) icon.

      The Edit Form Field - Create Machine Catalog Item dialog box appears.

   b On the **Constraints** tab, from the **Value** drop-down list, select **Constant** and click **Add**.

   c In the Select Values dialog box, navigate to the blueprint under **Catalog**, select the check box next to the name of the blueprint, and click **Submit**.

   d Edit the field again, and on the **Constraints** tab, from the **Visible** drop-down list, select **Constant**, select **No**, and click **Submit**.

7 On the **Blueprint Form** tab, click **Next**.

8 On the **Provisioned Resource** tab, select **desktop[ViewDesktop]** and click **Add**.

   The blueprint appears on the **Service Blueprints** page and the Status column shows that the blueprint is in draft form.

9 On the **Service Blueprints** page, select the blueprint and click the **Publish** button above the table.

Results

The service blueprint for the workflow is published and appears in the **Advanced Services > Service Blueprints** table.

What to do next

Import other workflows.

Import the Advanced Desktop Allocation Workflow

This workflow enables a delegated administrator to allocate machines to an end user, selecting either **Horizon View** or **vRealize Automation** as the machine provider.

Procedure

1 Log in to vRealize Automation as an administrator.

2 To select a new Service Blueprint, select **Design > XaaS > XaaS Blueprints**.

3 Click the **Add** (+) icon.

4 On the **Add Blueprint - Workflow** tab, navigate to **Library > Horizon > Workflows > vCAC**, select the workflow, and click **Next**.

5 On the **Details** tab, select the **Hide catalog request information page** check box and click **Next**.

6 (Optional) On the **Blueprint Form** tab, bind the **Create Machine Catalog Item** field to a specific machine blueprint.

   Performing this task means that the end user or delegated administrator cannot navigate through the catalog of blueprints to select a blueprint. As a security measure, you can configure the workflow so that the blueprint is already selected.

   a On the **Blueprint Form** tab, click in the **Create Machine Catalog Item** text box and click the **Edit** (pencil) icon.

      The Edit Form Field - Create Machine Catalog Item dialog box appears.

   b On the **Constraints** tab, from the **Value** drop-down list, select **Constant** and click **Add**.

   c In the Select Values dialog box, navigate to the blueprint under **Catalog**, select the check box next to the name of the blueprint, and click **Submit**.

   d Edit the field again, and on the **Constraints** tab, from the **Visible** drop-down list, select **Constant**, select **No**, and click **Submit**.

7 On the **Blueprint Form** tab, click **Next**.

8 On the **Provisioned Resource** tab, verify that no items are selected and click **Add**.

Note Verify that **desktop[ViewDesktop]** is not selected. That resource applies only to the self-service workflows and not to the Advanced Desktop Allocation workflow.

The blueprint appears on the **Service Blueprints** page and the Status column shows that the blueprint is in draft form.

9 On the **Service Blueprints** page, select the blueprint and click the **Publish** button above the table.

Results

The service blueprint for the workflow is published and appears in the **Advanced Services > Service Blueprints** table.

Import the Assign an AppStack to User Workflow

This workflow enables end users to request an application stack for their own use.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Click the **Design** tab.

3 To add a blueprint for the workflow, select **Xaas > XaaS Blueprints** and click the **New (+)** button.

4 On the **Workflow** tab on the New Blueprint pane, select **Orchestrator > Library > Horizon > Workflows > vCAC**.

5 Select the **Assign an App Stack to User** workflow and click **Next**.

6 In the **Assign an App Stack to User - Edit Blueprint** pane, delete the default value in the **Name** text box, and enter `Self Service to Request an App Stack`.

7 Select the **Hide catalog request information page** check box and click **Next**.

8 On the **Blueprint Form** tab, click in the **The User to Entitled** text box.

9 Click the **Constraints** tab and specify the constraint values to use for the user.

   a Click to expand the **Value** drop-down menu and select the **Field** radio button.

   b Click the **Define Field Values** link, expand **Request Info > Requested by**, and select **Principal ID** from the drop-down menu.

   c To save your selection, click **Apply**.

   d On the **Constraints** tab, click to expand the **Visible** drop-down menu, select **Constant**, and select **No**.

   e Click **Apply**.

10 On the **Blueprint Form** tab, click **Finish**.

   The new Self-Service to Request an AppStack blueprint appears on the **XaaS Blueprints** page and has a status of Draft.

11 Select the row for the Self-Service to Request an AppStack blueprint and click the **Publish** button above the table.

Results

The service blueprint for the Self-Service to Request an AppStack workflow is published and appears in the **Xaas > Xaas Blueprints** page.

Import the Self-Service Remote Application Workflow

This workflow enables end users to request a remote application for their own use.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Click the **Design** tab

3 Select **Xaas > XaaS Blueprints** and click the **New (+)** button to add a blueprint for the workflow.

4 On the **Workflow** tab on the New Blueprint pane, select **Orchestrator > Library > Horizon > Workflows > vCAC**.

5 Select the **Self-Service Request Application** workflow and click **Next**.

6 In the **Self-Service Request Application – Edit Blueprint** pane, select the **Hide catalog request information page** check box and click **Next**.

7 On the **Blueprint Form** tab, click **Next**.

8 On the **Provisioned Resource** tab, click **Finish**.

   The new Self-Service Request Application blueprint appears on the **XaaS Blueprints** page and has a status of Draft.

9 Select the row for the Self-Service Request Application blueprint and click the **Publish** button above the table.

Results

The service blueprint for the Self-Service Request Application workflow is published and appears in the **Xaas > Xaas Blueprints** table.

Import the Port Pool to vCAC Workflow

This workflow enables a delegated administrator to import desktop pools into vRealize Automation and manage the pools directly from the vRealize Automation console.

Procedure

1 Log in to vRealize Automation as an administrator.

2 Add a blueprint for the workflow.

   a In the workflows hierarchical list, select **Library > Horizon > Configuration > vCAC**.

   b Right-click the **Add or Update Port Pool to vCAC** workflow and select **Start workflow**.

3 On the **Details** tab, select the **Hide catalog request information page** check box and click **Next**.

4 On the **Blueprint Form** tab, edit the **vCACUser** field to bind the blueprint to a user.

   a Click in the **vCACUser** text box and click the **Edit** (pencil) icon.

   b In the Edit Form Field - vCACUser dialog box, click the **Constraints** tab.

   c Click to expand the **Value:** drop-down list.

   d Select the **Field** radio button and click to expand the **Request Info** item.

   e Click to expand the **Requested by** item and select **Principal ID**.

   f Click to expand the **Visible:** drop-down list.

   g To hide this parameter in catalog request, select the **Constant** radio button, and select **No**.

   h Click **Submit**.

5 On the **Blueprint Form** tab, click **Next**.

6 On the **Provisioned Resource** tab, select **pool[ViewPool]** and click **Add**.

   The blueprint appears on the **Service Blueprints** page and the Status column shows that the blueprint is in draft form.

7 On the **Service Blueprints** page, select the blueprint and click the **Publish** button above the table.

Results

The service blueprint for the workflow is published and appears in the **Advanced Services > Service Blueprints** table.

What to do next

If you have not already added a service to make the workflows available for delegated administrators or end users, perform the procedure described in Configure the Catalog Item for the Workflow.

Entitle users to the actions that vRealize Automation displays for desktop and pool items. See Entitle Users to Action Items.

Entitle Users to Action Items

After you create action items, you can entitle end users and delegated administrators to use the action buttons on the **Items** tab of vRealize Automation.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have created entitlements so that delegated administrators and end users can use services. See Create Entitlements for Delegated Administrators and End Users.
- Create service blueprints for the appropriate workflows. See Import Workflows for Desktop and Pool Management.

Procedure

1. Log in to vRealize Automation as an administrator.
2. Click the **Administration** tab.
3. Select **Catalog Management > Entitlements**.
4. Click the appropriate item in the list on the **Entitlements** page.

   You have already created entitlements for services, and now you are adding entitlements for actions.
5. On the **Items & Approvals** tab, click the **Add** (+) icon for **Entitled Actions**.
6. In the Add Actions to Entitlement dialog box, from the **Type** drop-down list, select **ViewPool** or **ViewDesktop**, as appropriate.

   If you are editing a delegated administrator entitlement, select **ViewPool**. If you are editing an end user entitlement, select **ViewDesktop**.
7. Select the check boxes next to the names of the appropriate actions and click **OK**.

   The actions are added to the **Entitled Actions** list.
8. On the **Edit Entitlement** page, click **Update**.
9. Repeat the process as necessary so that both end users and delegated administrators have the correct action entitlements.

What to do next

Import icons that will be displayed on the **Items** tab for end users and delegated administrators in vRealize Automation. See Import Action Icons into vRealize Automation.

Import Action Icons into vRealize Automation

You can upload the action icons that you exported from vRealize Orchestrator and saved to your local computer.

Prerequisites

- Verify that you exported the icons to your local system. See Export Action Item Icons from vRealize Orchestrator.
- Entitle users to the actions that appear for desktop and pool items in vRealize Automation. See Entitle Users to Action Items.

Procedure

1. Log in to vRealize Automation as an administrator.
2. Click the **Administration** tab.
3. Select **Catalog Management > Actions**.
4. On the **Actions** page, expand the **Advanced Search** control, and in the **Resource Type** drop-down menu, select **ViewDesktop** or **ViewPool**, and click the search icon.

   Only the actions for this type of resource appear.
5. Click the appropriate item in the list of filtered actions and click **Browse** next to **Icon**.
6. Navigate to the icon file on your local computer, select the file, and click **Open**.
7. On the **Configure Action** page, click **Update**.

Results

The icon appears on the **Items** tab in vRealize Automation.

Creating Machines and Managing Pools in vRealize Automation

6

You can run workflows that add a vRealize Automation-provisioned machine to a desktop pool.

If you use vRealize Automation machine blueprints to create virtual machines, you can manage the virtual machines from the **Infrastructure** tab of vRealize Automation, which provides actions such as reboot, shut down, and destroy. vRealize Automation also provides advanced policies for such things as number of lease days, cost, and archive days.

This chapter includes the following topics:

- Prerequisites for Creating Machines in vRealize Automation
- Create Templates and Blueprints for Adding Machines to Desktop Pools
- Use Machine Blueprints to Create and Add Desktops to Pools
- Configure a Machine Blueprint Service for Advanced Desktop Allocation
- Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users
- Deleting Machines Provisioned by vRealize Automation

Prerequisites for Creating Machines in vRealize Automation

You must run certain vCloud Automation Center plug-in workflows, and certain Horizon configuration workflows, before you can use vRealize Automation to create machines for desktop pools.

You must perform the following tasks before you can run the Configure vCAC Blueprint to Provision Machine to Pool workflow, the Self-Service Advanced Desktop Allocation workflow, or the Advanced Desktop Allocation workflow.

1. Log in to the vRealize Orchestrator Configuration interface as an administrator and verify that the vRealize Automation (vCAC) plug-in is installed.

   If you are using an vRealize Orchestrator instance that is embedded in vRealize Automation, this plug-in is already installed.

2. Log in to vRealize Orchestrator as an administrator and run the Add a vCAC Host workflow in the `vRealize Automation/Configuration` folder.

You can use the default settings for all items, except that for **Session mode**, you must select **Shared Session** from the drop-down menu. The Authentication user name and password are the credentials for the tenant administrator.

3 To run the following workflow, add the IaaS Host of a vRA Host workflow in the `vRealize Automation/Configuration` folder.

   You can use the default settings for all items, except that for **Session mode**, you must select **Shared Session** from the drop-down menu. The Authentication user name and password are local administrator credentials for logging in to the Windows operating system of that virtual machine.

4 Run the Install vCO Customization workflow in the `vRealize Automation/Infrastructure Administration/Extensibility/Installation` folder.

   On the **Stubs** page of the wizard, set the **WFStubMachineProvisioned** and **WFStubUnprovisionMachine** to **Yes**.

5 Add guest credentials by running the Add Guest Credentials workflow of the vRealize Orchestrator Plug-in for Horizon plug-in.

   This workflow is in the `Horizon/Configuration/Horizon Registration Configuration` folder. The guest credentials are the user name and password for logging in as an administrator or domain administrator on the virtual machine.

6 To enable the delegated administrator to use the guest credentials and have access to the data center and virtual machine folders, run the Manage Delegated Administrator Configuration for Registration workflow in the `Horizon/Configuration/Horizon Registration Configuration` folder.

7 To enable end users to use the guest credentials and have access to the data center and virtual machine folders, run the Manage Self Service Configuration for Registration workflow in the `Horizon/Configuration/Horizon Registration Configuration` folder.

Create Templates and Blueprints for Adding Machines to Desktop Pools

After you create and configure machine blueprints, you can select a blueprint in the Configure vCAC Blueprint to Provision Machine to Pool workflow, the Advanced Desktop Allocation workflow, or the Self-Service Advanced Desktop Allocation workflow.

Prerequisites

- Run the vRealize Orchestrator workflows described in Prerequisites for Creating Machines in vRealize Automation.
- Log in to vRealize Automation as a tenant administrator and verify that an endpoint has been created for vRealize Orchestrator and that its priority is set to **1**.

On the **Infrastructure** tab, select **Endpoints > Endpoints**, verify that vRealize Orchestrator appears in the list of endpoints, and verify that the endpoint has the **VMware.VCenterOrchestrator.Priority** property set to **1**. For more information, see "Create a vRealize Orchestrator Endpoint" in the *vRealize Automation Machine Extensibility* document.

- If you plan to make action buttons available on the **Items** tab of vRealize Automation so that delegated administrators can use action buttons to perform pool management tasks, perform the tasks described in Chapter 5 Making Desktop and Pool Actions Available in vRealize Automation.
- Become familiar with the Information as a Service (IaaS) concepts and the process of creating machine blueprints and creating services and entitlements. For information, see the vRealize Automation documentation.

Procedure

1 Log in to vRealize Automation as a tenant administrator and create one or more machine blueprints that have a source type of `iaas-service`.

Note When specifying the machine name in the blueprint, use a naming scheme that indicates that the machine was created in vRealize Automation. To delete machines that were created in vRealize Automation, use vRealize Automation. The naming scheme enables an administrator identify the machine. Do not delete the machine in Horizon Console. If the machine is deleted in Horizon Console, the machine status in vRealize Automation appears as **Missing**.

2 When you create the virtual machine template, install the latest version of VMware Tools and Horizon Agent in the guest operating system.

3 When you create the virtual machine template, add the machine to the domain.

4 If you are creating a blueprint for an unmanaged machine, verify that the blueprint contains a customization specification that configures the virtual machine so that it has a unique host name.

Got to the **Build Information** tab of the blueprint properties and verify that the **Customization spec** text box specifies which customization spec to use.

If the provided customization spec is not set up to appropriately, the machine might remain in the status of `Customizing` for over an hour before failing.

5 Publish the machine blueprint.

6 To create a service for the blueprint, select **Administration > Catalog Management > Services** and enter information in the wizard.

For example, you can create a specific service for machine blueprints rather than using the service that you created for service blueprints.

What to do next

Add the appropriate entitlement and run the appropriate workflow. See Use Machine Blueprints to Create and Add Desktops to Pools and Configure a Machine Blueprint Service for Advanced Desktop Allocation.

Use Machine Blueprints to Create and Add Desktops to Pools

Administrators can run the Configure vCAC Blueprint to Provision Machine to Pool workflow to create managed or unmanaged machines in vRealize Automation and add the machines to a specific manual desktop pool.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Perform the appropriate tasks from the topic Exposing vRealize Orchestrator Plug-in for Horizon Workflows in vRealize Automation. These tasks include creating business groups and services for delegated administrators and end users, creating entitlements for the services, configuring catalog items, and binding certain text boxes to specific values.
- Run the vRealize Orchestrator workflows described in Prerequisites for Creating Machines in vRealize Automation.
- Create one or more machine blueprints as described in Create Templates and Blueprints for Adding Machines to Desktop Pools.
- If you plan to make action buttons available on the **Items** tab so that delegated administrators can use action buttons to perform pool management tasks, perform the tasks described in Chapter 5 Making Desktop and Pool Actions Available in vRealize Automation.

Procedure

1. Log in to vRealize Automation as a tenant administrator.
2. Add an entitlement for the delegated administrator.
   a. On the **Administration** tab, select **Catalog Management > Entitlements** and click the item in the list for delegated administrators.
   b. Add the machine blueprint service to the **Entitled Services** list.
   c. If the delegated administrator can delete machines from specific pools, add a Destroy action to the **Entitled Actions** list and select **Virtual Machine** for **Type**.
   d. After adding the entitlements, click **Update**.

3 Log in to vRealize Orchestrator as an administrator and run the Configure vCAC Blueprint to Provision Machine to Pool workflow in the `Horizon/Configuration` folder.

   You can select the blueprint from the **Blueprints** folder of the IaaS host of the vCAC host.

   Some custom properties are added to the blueprint.

4 Navigate to **Design > Blueprints > Blueprints**, edit the blueprint, and view the custom properties on the **Properties** tab.

   If the blueprint is for a pool of unmanaged machines, you can see a **Credential Name** property. Do not edit the **ExternalWFStubs.MachineProvisioned** and **ExternalWFStubs.UnprovisionMachine** properties. These properties indicate the IDs of the workflows.

5 To troubleshoot an unsuccessful workflow run, in vRealize Orchestrator, navigate to **Horizon > CoreModules > Business Logic** and select the appropriate workflow to view its logs.

Action	Workflow Name
Add managed machines.	`add-vcac-machine-to-managed-pool`
Add unmanaged machines.	`add-vcac-machine-to-unmanaged-pool`
Delete a managed machine.	`remove--vcac-machine-to-managed-pool`
Delete an unmanaged machine.	`remove-vcac-machine-to-unmanaged-pool`

Results

The blueprint appears on the **Catalog** tab for the delegated administrator. If the IaaS administrator has configured the blueprint so that delegated administrators can change the number of CPUs, amount of memory, and gigabytes of hard disk space for the machine, the delegated administrator can make these changes on the **Request Information** tab when submitting the request. The delegated administrator can also change the number of machines to provision. The delegated administrator can monitor the progress of machine creation by clicking the **Requests** tab.

After the request succeeds, the delegated administrator can go to the **Items** tab, click **Machines** in the left panel, and see the machine or machines listed on the right panel. The delegated administrator can click a machine name to access the actions that are available, such as **Destroy**. The pod and pool name are available on the **Properties** tab.

Configure a Machine Blueprint Service for Advanced Desktop Allocation

Administrators can run the Advanced Desktop Allocation workflow or the Self-Service Advanced Desktop Allocation workflow to enable delegated administrators and end users to create managed or unmanaged machines in vRealize Automation, add the machine to a specific manual desktop pool, and assign the desktop to a specific user.

The goal of this procedure is to configure a blueprint service so that delegated administrators and end users can request to create desktop items that appear on the **Items** tab in vRealize Automation. End users can perform desktop management actions.

Prerequisites

- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Perform the appropriate tasks listed in Exposing vRealize Orchestrator Plug-in for Horizon Workflows in vRealize Automation. These tasks include creating business groups and services for delegated administrators and end users, creating entitlements for the services, configuring catalog items, and binding certain text boxes to specific values.
- Run the vRealize Orchestrator workflows described in Prerequisites for Creating Machines in vRealize Automation.
- Create one or more machine blueprints as described in Create Templates and Blueprints for Adding Machines to Desktop Pools.

  Note Do not use a blueprint that was already selected when running the Configure vCAC Blueprint to Provision Machine to Pool workflow. That workflow adds properties to the blueprint that must not be present for this procedure.

- Perform the task Import Desktops and Pools as Custom Resources.
- If you plan to make action buttons available on the **Items** tab so that end users can use action buttons to perform desktop management tasks, perform the tasks described in Chapter 5 Making Desktop and Pool Actions Available in vRealize Automation.

Procedure

1. Log in to vRealize Automation as a tenant administrator.
2. Add the tenant administrator to the delegated administrators entitlement.

   a. On the **Administration** tab, select **Catalog Management > Entitlements** and click the item in the list for delegated administrators.

   b. On the **Details** tab, in the **Users & Groups** list, add the tenant administrator to the entitlement.

   c. On the **Items & Approvals** tab, add the machine blueprint service to the **Entitled Services** list.

   d. Add a **Destroy** action to the **Entitled Actions** list.

      For **Type**, select **Virtual Machine**.

   e. When you are finished adding these entitlements, click **Update**.

3 If you plan to use the Advanced Desktop Allocation workflow, configure provisioning.

   a Select **Design > Service Blueprints**.

   b Click **Advanced Desktop Allocation**, and, on the **Provisioned Resources** tab, select **No provisioning**.

   c Click **Update**.

4 If you plan to use the Self-Service Advanced Desktop Allocation workflow, configure provisioning.

   a Select **Advanced Services > Service Blueprints**.

   b Click **Self-Service Advanced Desktop Allocation**, and, on the **Provisioned Resources** tab, select **Desktop [ViewDesktop]**.

   c Click **Update**.

5 On the **Catalog** tab, click the service that you created for machine blueprints and verify that the machine blueprints appear in the panel on the right.

Results

Items appear on the vRealize Automation **Catalog** tab so that delegated administrators and end users can request desktops. For descriptions of the possible scenarios that the Advanced Desktop Allocation workflows enable, see Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users.

Advanced Desktop Allocation Scenarios for Delegated Administrators and End Users

After administrators perform the required configuration tasks, delegated administrators and end users can run the advanced desktop allocation workflows to accomplish various desktop and pool management goals.

For end users, the action items described in the following scenarios appear when the user clicks a desktop item on the user's **Item Details** tab in vRealize Automation. These desktop management actions can include start (the virtual machine), log out, reboot, shut down, and recycle. For linked-clone desktops, users can also use a refresh action to revert the machine back to the state that it was in when the user first acquired the machine.

For delegated administrators, the action items described in the following scenarios appear when the delegated administrator clicks a desktop pool item on the **Item Details** tab. These pool management actions can include drop pool (delete the pool), manage assignment (of the desktop), manage entitlement (to the desktop pool), manage session, and, for linked-clone pools, recompose.

Advanced Desktop Allocation Workflow Scenario: The Delegated Administrator Wants to Provision a Machine for an End User and Add It to a Pool

1. Delegated administrators can run the Advanced Desktop Allocation workflow from vRealize Orchestrator, vRealize Automation, or vSphere Web Client. When the workflow runs, the workflow calls the `vcac-desktop-callback-bl` (business logic) workflow.
2. The workflow checks whether a machine exists and whether the specified user is already entitled to the machine.
   - If the machine exists and the user is entitled to the pool and assigned to the machine, the workflow takes no action but reports success.
   - If the machine exists and the user is assigned to it, but the user is not entitled to the pool, the workflow entitles the user to the pool.
   - If the machine does not exist, the workflow runs two times. The first time the workflow runs, the machine is created, and the user is assigned to it. The second time the workflow runs, the user is entitled to the pool.
3. Primary administrators and delegated administrators can monitor the progress of the workflow in vRealize Orchestrator or vRealize Automation.
   - In vRealize Orchestrator, the administrator can select **Horizon > CoreModules > Business Logic** and select the `vcac-desktop-callback-bl` workflow.
   - In vRealize Automation, tenant administrators and delegated administrators can see a request created on the **Requests** tab. Tenant administrators can also select **Infrastructure > Machines > Managed Machines** and watch the machine get added to the list. The status changes from `InitializingRequest` to `CloneMachine` to `MachineProvisioned` to `On`.
   - In Horizon Console, the machine appears in the list of machines that belong to the specified desktop pool. The status changes from `Waiting for Agent` to `Available`. An entitlement for the user appears in the list of entitlements.
4. After the workflow succeeds, the end user can log in to vRealize Automation, click the **Items** tab, and click **Machines** to see the machine. Because vRealize Automation provisioned the machine, the machine appears in the **Machines** panel rather than in the **Horizon** panel.

Self-Service Advanced Desktop Allocation Workflow Scenarios

For desktop items, users can click the item to go to the **Item Details** tab and see the status of the remote desktop. Users can determine whether the machine is connected, powered on, in an error state, or undergoing a recompose operation.

Scenario 1: The End User Has a Machine Item Listed Under Machines Rather Than Horizon

For the first scenario, the delegated administrator has run the Advanced Desktop Allocation workflow to create and provision a machine in vRealize Automation and assign it to an end user. The end user has an item for the machine on the **Items** tab in vRealize Automation. The machine is listed only in the **Machines** panel, and the user wants the item to appear in the **Horizon** panel, so that the user can access the desktop management action buttons.

1 The end user goes to the **Catalog** tab in vRealize Automation and runs the Self-Service Advanced Desktop Allocation workflow, selecting **vRealize Automation Center** as the machine provider.

2 Because the machine exists and is allocated to the user, the workflow reports success and places an item for the machine on the end user's **Horizon** panel.

3 The machine appears on the user's **Horizon** panel, and the user can access action buttons such as **Start**, **Recycle**, and **Logoff**.

Scenario 2: The End User Has a Horizon Desktop but Wants to Manage It in vRealize Automation

For the second scenario, the end user has a machine that was provisioned and assigned to the user in Horizon Console. No items appear in the user's **Items** tab in vRealize Automation. The end user wants to create an **Items** tab machine item in the **Horizon** panel, so that the user can access the desktop management action buttons.

1 The end user clicks the **Catalog** tab in vRealize Automation and runs the Self-Service Advanced Desktop Allocation workflow, selecting **Horizon View** as the machine provider.

2 Because the machine exists in a desktop pool and is allocated to the user, the workflow reports success and places an item for the machine on the end user's **Horizon** panel.

3 The end user can go to the **Horizon** panel and access action buttons such as **Start**, **Recycle**, and **Logoff**.

Scenario 3: Then End User Wants a Machine and Wants to Manage It in vRealize Automation

For the third scenario, no machine was created for the end user, either in vRealize Automation or in Horizon Console. The end user wants to have a machine created, provisioned, assigned, and entitled to the user. The end user also wants to create an **Items** tab machine item in the **Horizon** panel, to access the desktop management action buttons.

1 The end user selects the **Catalog** tab in vRealize Automation and runs the Self-Service Advanced Desktop Allocation workflow, selecting **vRealize Automation Center** as the machine provider.

2 Because a machine does not exist, the machine is created, provisioned, added to the specified pool, and allocated to the user. The user is entitled to the pool. The workflow reports success. The workflow places an item for the machine on the end user's **Machines** panel.

3 Primary administrators can monitor the progress of the workflow in Orchestrator or in vRealize Automation. End users can monitor requests in vRealize Automation.

   - In vRealize Orchestrator, the administrator can view the logs of the workflow run.
   - In vRealize Automation, delegated administrators, tenant administrators, and end users can see a request created on the **Requests** tab. Tenant administrators can also select **Infrastructure > Machines > Managed Machines** and see the machine added in the list. The status changes from `InitializingRequest` to `CloneMachine` to `MachineProvisioned` to `On`.
   - In Horizon Console, the machine appears in the list of machines that belong to the specified desktop pool. The status changes from `Waiting for Agent` to `Available`. An entitlement for the user appears in the list of entitlements.

4 The machine also appears on the user's **Horizon** panel, and the user can access action buttons such as **Start**, **Recycle**, and **Logoff**.

Deleting Machines Provisioned by vRealize Automation

When deleting machines that were created and provisioned through the vRealize Automation service catalog, as a best practice, use a workflow or the Destroy action available in vRealize Automation, rather than deleting the machine through Horizon Console or vSphere Web Client.

If a vRealize Automation-provisioned machine is deleted in Horizon Console, the machine status on the **Infrastructure** tab in vRealize Automation appears as **Missing**. For this reason, consider using a machine-naming convention that indicates whether the machine provider is vRealize Automation or VMware Horizon.

If this situation occurs, use the Destroy action on the **Infrastructure** tab in vRealize Automation. Whenever an administrator or delegated administrator uses the Destroy action, the virtual machine is removed from the desktop pool and the virtual machine is deleted.

To use the Destroy action, the tenant administrator or delegated administrator must have delegated administrator access on the pool to which the machine belongs. To add a tenant administrator or delegated administrator to the group of delegated administrators for the pool, run the Add Delegated Administrator Configuration workflow as described in Assign Delegated Administrators to Pools. To determine the pool to which a machine belongs, select the **Properties** tab for the machine on the **Infrastructure** tab in vRealize Automation.

When you use the Destroy action, the vcac-desktop-callback workflow runs in vRealize Orchestrator. This workflow is in the `Horizon/CoreModules/Business Logic` folder. To monitor the action, you can log in to vRealize Orchestrator and view the logs for the workflow. You can also monitor progress in vRealize Automation, by clicking the machine item on the **Infrastructure > Machines > Managed Machines** tab. The status changes from `InitializingRequest` to `UnprovisioningMachine` to `Disposing`. Finally, the machine is removed from the list.

Note For delegated administrators, the Destroy action might also be available on the **Items** tab, from the **Machines** panel. The delegated administrator can click a machine name to access the **Item Details** tab, where the **Destroy** button might be available. The **Recycle** button, which is available only for end users, removes the user's entitlement to the pool and unassigns the user from the machine. It does not delete the machine unless the pool policy is set to do so.

Working with Unmanaged Machines

7

For manual unmanaged pools in VMware Horizon, the Connection Server instance is not able to obtain information from a vCenter Server instance. The unmanaged machines must be registered with the Connection Server instance before they can be added to a desktop pool.

Prerequisites for Adding Unmanaged Machines to Pools applies to all types of unmanaged machines. The other topics apply only to physical machines that you add to a desktop pool.

This chapter includes the following topics:

- Prerequisites for Adding Unmanaged Machines to Pools
- Adding Physical Machines and Non-vSphere Virtual Machines to Pools

Prerequisites for Adding Unmanaged Machines to Pools

Use this check list to verify that you have performed all the tasks required to run the appropriate workflow for adding the machine to a manual unmanaged pool.

Separate workflows are available to enable a delegated administrator to add physical and virtual machines to manual desktop pools in VMware Horizon.

- Use the Add Unmanaged Machines to Pool workflow for unmanaged machines that a vCenter Server instance manages, but the vCenter Server instance is not added to VMware Horizon.
- To add physical machines and non-vSphere virtual machines, such as machines that you create by using Citrix XenServer or VMware Workstation, use the Add Physical Machines to Pool workflow in the `Workflows/Example` folder. Alternatively, you can run the other workflows as described in Adding Physical Machines and Non-vSphere Virtual Machines to Pools.

Before you run a workflow for adding unmanaged machines to a pool, verify that you have performed the following tasks:

- Add guest credentials by running the Add Guest Credentials workflow of the vRealize Orchestrator Plug-in for Horizon plug-in.

  This workflow is in the `Configuration/Horizon Registration Configuration` folder. The guest credentials must be for logging in as an administrator or domain administrator on the virtual machine.

- To enable the delegated administrator to use the guest credentials and access the data center and virtual machine folders, run the Manage Delegated Administrator Configuration for Registration workflow in the `Configuration/Horizon Registration Configuration` folder .
- To enable end users to use the guest credentials and access the data center and virtual machine folders, run the Manage Self Service Configuration for Registration workflow in the `Configuration/Horizon Registration Configuration` folder.
- For vSphere virtual machines, install the latest version of VMware Tools in the unmanaged virtual machine.

  For step-by-step instructions, see the VMware vSphere help.
- Install Horizon Agent in the unmanaged machine.

  For step-by-step instructions, see the *Setting Up Virtual Desktops in Horizon* document.
- If the unmanaged machine is a Windows Server machine, enable the server to be used as a remote desktop:

  a Log in to Horizon Console.

  Horizon Console uses a URL that has the format https://*connection-server*/admin.

  b Select **Settings > Global Settings**.

  c On the **General Settings** tab, click **Edit**.

  d Select the **Enable Windows Server desktops** check box and click **OK**.
- For vSphere virtual machines, configure the vCenter Server instance to use the **Share a unique session** option for managing user logins.

  Note The following steps assume that the connection to the vCenter Server instance has already been configured. If it is not yet configured, see "Configure the Connection to a vCenter Server Instance" in *Using VMware vRealize Orchestrator Plug-Ins*.

  a Log in to the vRealize Orchestrator configuration console.

  The configuration console uses a URL that has the format https://*vco-server*:8283.

  b Select **vCenter Server** and click **Edit** for the vCenter Server instance.

  c Under **Specify which strategy will be used for managing the users logins**, select **Share a unique session** and click **Apply changes**.

  d Restart the vRealize Orchestrator Server service.

The Add Unmanaged Machines to Pool workflow for vSphere virtual machines has some important limitations. See Add Unmanaged Machines to Pool.

For physical machines and non-vSphere virtual machines, you must perform additional configuration tasks. See Configure a Physical Machine for an Unmanaged Pool and Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines. You can run the Add Physical Machines to Pool workflow, available in the `Workflows/Example` folder, or run the Register Machines to Pool workflow and the PowerShell workflows described in Run Workflows to Add Physical Machines as PowerShell Hosts.

Adding Physical Machines and Non-vSphere Virtual Machines to Pools

You must perform several configuration tasks to add physical machines and non-vSphere virtual machines, such as machines created in Citrix XenServer, Microsoft HyperV, or VMware Workstation, to manual unmanaged desktop pools.

After you meet the requirements in Prerequisites for Adding Unmanaged Machines to Pools, you must complete the following tasks:

1. Enable Windows Remote Management, set remote execution policies, add the vRealize Orchestrator server as a trusted host, and enable communication with the PowerShell plug-in. For information, see Configure a Physical Machine for an Unmanaged Pool.
2. Configure the vRealize Orchestrator server to use Kerberos authentication. For information, see Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines.
3. Run the Add Physical Machines to Pool workflow in the `Workflows/Example` folder, or run the Register Machines to Pool workflow and run the PowerShell workflows described in Run Workflows to Add Physical Machines as PowerShell Hosts.

Configure a Physical Machine for an Unmanaged Pool

Before you add a physical machine to a manual unmanaged desktop pool, you must log in to the machine as an administrator and perform certain configuration tasks.

Prerequisites

- Verify that you have administrator credentials for logging in to the machine. If the machine is joined to a domain, obtain domain administrator credentials.
- Become familiar with the procedure for configuring WinRM to use HTTP. See the vCenter Plug-Ins documentation.

Procedure

1. Log in as an administrator and set the Windows Remote Manager service to start automatically.

   a. Go to the Services applet.

   b. Right-click the **Windows Remote Management (WS-Management)** service and select **Properties**.

   c. Select the startup type **Automatic**, click **Start**, and click **OK** after the service starts.

2. Start PowerShell as an administrator and use the following commands to configure remote execution policies.

   a. Use the following command to verify that the policy is set to `RemoteSigned`.

   ```
   Get-ExecutionPolicy
   ```

   b. If the policy is set to `Restricted`, use the following command:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   Press Y when prompted.

   c. Use the following command to enable remote execution for WinRM

   ```
   Enable-PSRemoting
   ```

   Press Y when prompted.

   d. Use a command to add vRealize Orchestrator hosts as trusted servers.

Option	Command
Add all machines as trusted hosts.	`Set-Item wsman:\localhost\client\trustedhosts *` or `set-item wsman:\localhost\Client\TrustedHosts -value *`
Add all domain machines as trusted hosts.	`set-item wsman:\localhost\Client\TrustedHosts *.`*domain*`.com`
Add a single machine (use the FQDN of the machine).	`set-item wsman:\localhost\Client\TrustedHosts -value` *hostname*`.`*domain*`.com`
Add a single machine using the IP address.	`set-item wsman:\localhost\Client\TrustedHosts -value` *xxx.xxx.xxx.xxx*

   Press Y when prompted.

   Note You can use the following command to see the list of trusted hosts:

   ```
   Get-item wsman:\localhost\Client\TrustedHosts
   ```

   e. Use the following command to restart WinRM Service:

   ```
   Restart-Service WinRM
   ```

3 On another Windows machine, test the connection to the machine you just configured by running the following command.

`Test-WsMan IP-or-DNS-of-machine`

For example: `Test-WsMan 12.34.56.78`

The output is similar to the following:

```
wsmid           : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor   : Microsoft Corporation
ProductVersion  : OS: 0.0.0 SP: 0.0 Stack: 2.0
```

If you use the following command, the output lists the contents of the C drive:

```
Invoke-Command -ComputerName IP-or-DNS-of-machine -ScriptBlock { Get-ChildItem C:\ }
-credential domain\administrator
```

4 Open a command prompt and configure the physical machine (WinRM host) to enable the communication with the PowerShell plug-in through the HTTP protocol.

If you use PowerShell 2.0, enclose the commands in single quotes, as follows:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'

winrm set winrm/config/client/auth '@{Basic="true"}'
winrm set winrm/config/client '@{AllowUnencrypted="true"}'
```

If the WinRM host machine is in an external domain, you must also run the following command to specify the trusted hosts:

```
winrm set winrm/config/client @{TrustedHosts="host1, host2, host3"}
```

You can use the following command to verify the settings after you finish making changes:

```
winrm get winrm/config
```

5 For machines that belong to a domain, enable and test Kerberos authentication.

a Open a command prompt and use the following commands to enable Kerberos authentication:

```
winrm set winrm/config/service/auth '@{Kerberos=”true”}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'

winrm set winrm/config/client/auth '@{Kerberos=”true”}'
winrm set winrm/config/client '@{AllowUnencrypted="true"}'
```

b Use the following command to test Kerberos authentication:

```
winrm id -r:machine.domain.com -auth:Kerberos -u:administrator@domain.com -p:'password'
```

6. Install Horizon Agent in the physical machine.

What to do next

Configure authentication on the vRealize Orchestrator server. See Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines.

Configure vRealize Orchestrator to Use Kerberos Authentication with Physical Machines

You must edit a configuration file on your vRealize Orchestrator server to specify the domain name and domain controller name.

Prerequisites

If you are using the vRealize Orchestrator virtual appliance, you must have the root password. If vRealize Orchestrator is installed in a Windows server, you must have the administrator credentials.

Procedure

1. Log in as root, or as an administrator if you have a Windows server.
2. Search for the `krb5.conf` file and rename it to `krb5.conf.back`.

   On a virtual appliance, this file is in the `etc/krb5.conf` folder, if it exists.
3. Create a `krb5.conf` file in the appropriate directory.

Server Type	Description
Virtual appliance	`/usr/java/jre-vmware/lib/security/`
Windows server	`C:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components\lib\security\`

4. In a text editor, edit the `krb5.conf` file and add the following lines, with the appropriate values.

```
[libdefaults]
   default_realm = YOURDOMAIN.COM
   udp_preference_limit = 1
[realms]
   YOURDOMAIN.COM = {
      kdc = yourDC.yourdomain.com
      default_domain = yourdomain.com
   }
[domain_realms]
.yourdomain.com= YOURDOMAIN.COM
yourdomain.com= YOURDOMAIN.COM
```

5 If you are using a virtual appliance, use the following command to change permissions of the file to make it readable.

```
chmod 644 /usr/java/jre-vmware/lib/security/krb5.conf
```

6 Verify that the PowerShell host (that is, the physical machine that must be registered) and the domain controller host names can be resolved from the vRealize Orchestrator server.

The DNS of the vRealize Orchestrator must be the same as the DNS of the domain controller, or you can add the machine names or IP addresses of the physical machines and domain controller to the `hosts` file on the vRealize Orchestrator server.

On a virtual appliance, this file is in the `/etc/hosts` folder.

7 Restart the vRealize Orchestrator Server service.

What to do next

Add physical machines as PowerShell hosts. See Run Workflows to Add Physical Machines as PowerShell Hosts.

Note As an alternative to running the PowerShell workflows, you can use the Add Physical Machines to Pool workflow in the `Workflows/Example` folder. This workflow combines the actions of the Register Machines to Pool workflow and the PowerShell workflows described in Run Workflows to Add Physical Machines as PowerShell Hosts. Before you run the Add Physical Machines to Pool workflow, you must perform the tasks described in Configure a Physical Machine for an Unmanaged Pool and Prerequisites for Adding Unmanaged Machines to Pools.

Run Workflows to Add Physical Machines as PowerShell Hosts

You must run PowerShell plug-in workflows to finish the process of adding physical machines and non-vSphere virtual machines to desktop pools by using the vRealize Orchestrator Plug-in for Horizon plug-in.

Note As an alternative to running the PowerShell workflows listed in this procedure and the Register Machines to Pool workflow, you can run the Add Physical Machines to Pool workflow in the `Workflows/Example` folder.

Prerequisites

- Verify that you have the vRealize Orchestrator Plug-In for Microsoft Windows PowerShell, which contains the workflows required for this procedure.
- Verify that you have administrator credentials for the vRealize Orchestrator server. The account must be a member of the vRealize Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.

- To register all machine DNS names into manual unmanaged desktop pools in VMware Horizon, run the Register Machines to Pool workflow. The Register Machines to Pool workflow returns a token, one for each registered DNS, that is pushed into the Windows Registry of the machines when you run the PowerShell command described in this procedure.

Procedure

1 Log in to vRealize Orchestrator as an administrator.

2 Click the **Workflows** view in vRealize Orchestrator.

3 In the workflows hierarchical list, select **Library > PowerShell > Configuration** and navigate to the **Add a PowerShell host** workflow.

4 Right-click the **Add a PowerShell host** workflow and select **Start workflow**.

5 Provide the host name and fully qualified domain name of the physical machine and click **Next**.

If the machine is not in a domain, you can use the IP address. If you do not supply the port number, the default port is used.

6 Enter values in the form that appears and click **Next**.

Option	Action
PowerShell remote host type	Select **WinRM** from the drop-down menu.
Transport protocol	Select **HTTP** from the drop-down menu.
Authentication	If the machine is in the domain, select **Kerberos** from the drop-down menu. If the machine is not in the domain, select **Basic**.

7 Enter values in the form that appears.

Option	Action
Session mode	Select **Shared session** from the drop-down menu.
User name	If the machine is in a domain, use the format `*administrator*@*domain*.com`. If the machine is not in a domain, use the user name of the local administrator account.

8 To run the workflow, click **Submit**.

9 When the workflow finishes, right-click the **Invoke a PowerShell Script** workflow in the `PowerShell` folder and select **Start workflow**.

10 Select the host that you added and click **Next**.

11 (Optional) Add the `Identity` registry key.

a Verify that the `hklm:\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Identity` registry key exists.

b If the registry key does not exist, enter the following command:

```
New–Item –Path "hklm:\SOFTWARE\VMware, Inc.\VMware VDM\Agent" –Name Identity
```

12 In the **Script** text area, enter the following command:

```
New–ItemProperty –Path "hklm:\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Identity" –Name Bootstrap –
PropertyType String -Value “TokenReturnedByWorkflow” -Force
```

For *TokenReturnedByWorkflow*, use the token returned by the Register Machines to Pool workflow that you previously executed to register machine DNS names.

13 To run the workflow, click **Submit**.

Results

The Horizon Agent token on the machine is now paired with the Connection Server instance.