Using the Horizon vCenter Orchestrator Plug-In

VMware Horizon 6 6.0

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

Using the Horizon vCenter Orchestrator Plug-In 5

1 Introduction to the Horizon vCenter Orchestrator Plug-In 7
- Role of the Horizon vCenter Orchestrator Plug-In 8
- Functionality Available with the Horizon vCenter Orchestrator Plug-In 8
- Horizon vCenter Orchestrator Plug-In Architecture 9
- Horizon vCenter Orchestrator Security Model 9
- Personas Used for Managing Workflows Across Distributed Organizations 10

2 Installing and Configuring the Horizon vCenter Orchestrator Plug-In 11
- Horizon vCenter Orchestrator Plug-In Functional Prerequisites 11
- Install or Upgrade the Horizon vCenter Orchestrator Plug-In 12
- Post-Upgrade Configuration Tasks 13
- Configure the Connection to a View Pod 14
  - Updating View Pod Connection Information 14
- Assigning Delegated Administrators to Desktop and Application Pools 15
  - Create a Delegated Administrator Role Using vSphere Web Client 15
  - Provide Access Rights to the Horizon vCenter Orchestrator Plug-In Workflows 16
  - Assign Delegated Administrators to Pools 17
- Best Practices for Managing Workflow Permissions 18
- Set a Policy for De-Provisioning Desktop Virtual Machines 19

3 Using Horizon vCenter Orchestrator Plug-In Workflows 21
- Access the Horizon vCenter Orchestrator Plug-In Workflow Library 21
- Horizon vCenter Orchestrator Plug-In Workflow Library 22
- Horizon vCenter Orchestrator Plug-In Workflow Reference 22
- Syntax for Specifying User Accounts in the Workflows 30

4 Making the Workflows Available in vSphere Web Client and vCloud Automation Center 31
- Exposing Horizon vCenter Orchestrator Plug-In Workflows in vSphere Web Client 32
  - Bind vSphereWebClient Workflows to Specific Pods and Pools in vCenter Orchestrator 32
  - Create Localized Versions of a Workflow for vSphere Web Client 33
- Exposing Horizon vCenter Orchestrator Plug-In Workflows in vCloud Automation Center 34
  - Create Business Groups for Delegated Administrators and End Users 35
  - Create Services for Delegated Administrators and End Users 35
  - Create Entitlements for Delegated Administrators and End Users 36
  - Bind vCAC60 Workflows to Specific Pods and Pools in vCloud Automation Center 37
  - Bind vCAC61 Workflows to a vCAC User 38
  - Make vCAC61 Self-Service Workflows Use Specific Pools 40
  - Configure Output Parameters for vCAC61 Workflows 41

Configure the Catalog Item for the Workflow 42

5 Working with Unmanaged Machines 43

Prerequisites for Adding Unmanaged Machines to Pools 43

Adding Physical Machines and Non-vSphere Virtual Machines to Pools 44

Configure a Physical Machine for an Unmanaged Pool 45

Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines 47

Run Workflows to Add Physical Machines as PowerShell Hosts 48

Index 51

Using the Horizon vCenter Orchestrator Plug-In

Using the Horizon vCenter Orchestrator Plug-In describes how to set up and start using the Horizon™ plug-in to VMware® vCenter Orchestrator™. The plug-in allows IT organizations to use VMware vCloud® Automation Center™ to automate the provisioning of desktops and applications that are provided by VMware Horizon™ (with View™).

Intended Audience

This information is intended for anyone who is installing and configuring the plug-in or who would like to automate and provision desktops and applications by using the workflow library. *Using the Horizon vCenter Orchestrator plug-in* is written for experienced users who are familiar with virtual machine technology, with Orchestrator workflow development, and with VMware Horizon 6.

Introduction to the Horizon vCenter Orchestrator Plug-In

1

The Horizon vCenter Orchestrator (vCO) plug-in allows interaction between vCenter Orchestrator and VMware Horizon 6. You can use this plug-in to expand the settings and methods for provisioning remote desktops and 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.

The workflows described in this document provide predefined, automated tasks that accomplish basic goals that are ordinarily performed in View Administrator or other View interfaces. View administrators can delegate access to the workflows to delegated administrators and end users, thereby increasing IT efficiency.

For end user enablement, the Horizon vCenter Orchestrator plug-in integrates with vCloud Automation Center to provide self-service access to applications and desktops. The plug-in workflows can be integrated with the request and approval processes that are built into the vCloud Automation Center service catalog, allowing end users to refresh their own desktops. End users can make requests that follow a standardized and auditable process that can result in immediate action, or they can direct their requests for administrative approval. For desktop environments where virtual machines must support rapid change and reuse, end users can provision desktops for themselves and de-provision, or recycle, the desktops to reduce waste of resources and capacity.

The Horizon vCenter Orchestrator plug-in provides an organized and manageable service catalog of functions that are entitled to appropriate users and groups, which increases IT efficiency. Automating and distributing tasks for delegated administration reduces the need for email correspondence and exception handling. The requests are routed into processes that are predefined and only flagged for approval if justification is needed. These standardized controls and processes allow administrators to deliver Desktops-as-a-Service (DaaS) with a one-to-many model of administration.

This chapter includes the following topics:

- "Role of the Horizon vCenter Orchestrator Plug-In," on page 8
- "Functionality Available with the Horizon vCenter Orchestrator Plug-In," on page 8
- "Horizon vCenter Orchestrator Plug-In Architecture," on page 9
- "Horizon vCenter Orchestrator Security Model," on page 9
- "Personas Used for Managing Workflows Across Distributed Organizations," on page 10

Role of the Horizon vCenter Orchestrator Plug-In

You must use the Orchestrator configuration interface to install and configure the Horizon vCenter Orchestrator plug-in. You use the Orchestrator client to run and create workflows and access the plug-in API.

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

Orchestrator allows integration with management and administration solutions through its open plug-in architecture. VMware Horizon 6 is one example of an administration solution that you can integrate with Orchestrator by using plug-ins.

Functionality Available with the Horizon vCenter Orchestrator Plug-In

The Horizon vCenter Orchestrator plug-in provides automation, self-service, and delegated administration for View environments. End users can perform self-service functions and delegated administrators can perform provisioning functions on behalf of end users.

The Horizon vCenter Orchestrator plug-in provides the following functions:

- Self-provision and de-provision, or recycle, machines through vCloud Automation Center in existing View desktop pools
- Self-service request and entitlement for applications through vCloud Automation Center
- Self-service request and entitlement for a desktop through vCloud Automation Center
- Self-service refresh of a machine through vCloud Automation Center
- Provision a machine into an existing desktop pool on behalf of an end user
- De-provision a machine on behalf of an end user and preserve the persistent disk if there is one
- Allow entitlement and assignment changes for application and desktop pools
- Allow modification of the minimum number of machines in a desktop pool, pool display name, and number of powered-on machines

With Horizon vCenter Orchestrator plug-in, the following functions have been added:

- Add managed virtual machines to manual desktop pools
- Add unmanaged virtual machines to manual unmanaged desktop pools
- Add physical machines to manual unmanaged desktop pools
- Allow session management for disconnecting, logging off, resetting, and sending messages to active View desktop sessions
- Provision multiple machines for multiple users
- Perform maintenance mode operations on View machines

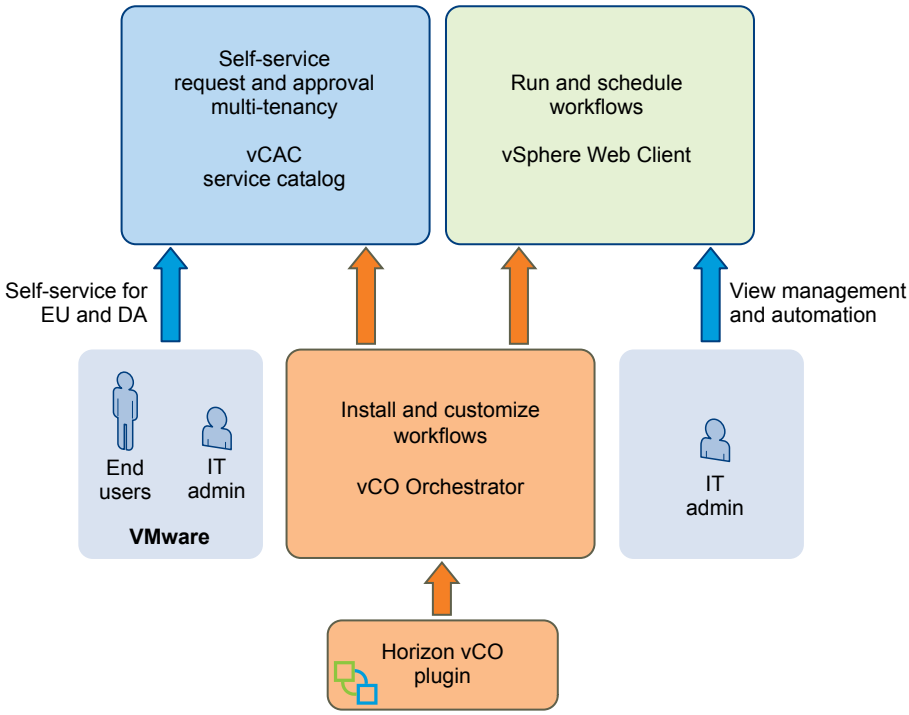
Horizon vCenter Orchestrator Plug-In Architecture

vCenter Orchestrator and vCloud Automation Center provide the architecture that supports the Horizon vCenter Orchestrator plug-in functions.

vCenter Orchestrator plug-ins allow seamless automation between the software environment in which the workflows are executed and the products with which the workflows interact. With the Horizon vCenter Orchestrator plug-in, workflows can be exposed natively, through the vSphere Web Client, to delegated administrators, and through the vCloud Automation Center service catalog. Although entitlement, scheduling, and execution of workflows are exposed through the vSphere Web Client and vCloud Automation Center, you can customize and configure the workflows only in the vCenter Orchestrator client.

The following diagram illustrates the Horizon vCenter Orchestrator plug-in architecture.

Figure 1-1. Horizon vCenter Orchestrator Plug-In Architecture



Horizon vCenter Orchestrator Security Model

The Horizon vCenter Orchestrator plug-in uses a trusted account security model. The administrator provides the credentials to the initial configuration between the View pod and the plug-in, and that trusted account is the security context that all workflows use between vCenter Orchestrator and VMware Horizon 6.

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

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

- Administrators use the vCenter Single Sign-On implementation to allow access by users or groups to run workflows within vSphere Web Client.

- Administrators use the service catalog and entitlement mechanisms within vCloud Automation Center to manage which workflows are exposed to specific users and groups.

Personas Used for Managing Workflows Across Distributed Organizations

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

Administrator

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

Delegated Administrator

The role and responsibilities of the delegated administrator (DA) are delegated by the administrator. For example, the delegated administrator can perform certain actions on certain desktop or application pools but not on others. Delegated administrators cannot change the scope for which they have been granted responsibility. The functions granted to the delegated administrator can span a wide spectrum, from provisioning multiple virtual machine desktops to very simple tasks, such as resetting desktops. Delegated administrators have the ability to act on behalf of multiple users. This power is a key to enabling administrative efficiency.

End User

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

Installing and Configuring the Horizon vCenter Orchestrator Plug-In 2

Installing the Horizon vCenter Orchestrator plug-in is similar to installing other vCenter Orchestrator plug-ins. Configuring the plug-in involves running various configuration workflows to connect to View components and to configure roles and permissions.

This chapter includes the following topics:

- "Horizon vCenter Orchestrator Plug-In Functional Prerequisites," on page 11
- "Install or Upgrade the Horizon vCenter Orchestrator Plug-In," on page 12
- "Post-Upgrade Configuration Tasks," on page 13
- "Configure the Connection to a View Pod," on page 14
- "Assigning Delegated Administrators to Desktop and Application Pools," on page 15
- "Best Practices for Managing Workflow Permissions," on page 18
- "Set a Policy for De-Provisioning Desktop Virtual Machines," on page 19

Horizon vCenter Orchestrator Plug-In Functional Prerequisites

The Horizon vCenter Orchestrator plug-in acts as middleware between Horizon 6, vCenter Orchestrator, and vCloud Automation Center. To be able to install and use the Horizon vCenter Orchestrator plug-in, your system must meet certain functional prerequisites.

VMware Horizon 6 (with View)

You must have access to a View Connection Server 6.0 or 6.0.1 instance. The Horizon vCenter Orchestrator plug-in works with VMware Horizon 6.

For more information about setting up VMware Horizon 6 (that is, 6.0 or 6.0.1), see the *View Installation* and *View Administration* documents, available from the documentation page at https://www.vmware.com/support/pubs/view_pubs.html.

vCenter Orchestrator

Verify that you have a running instance of Orchestrator. You can log in to the Orchestrator configuration interface at http://*orchestrator_server*:8283. The Horizon vCenter Orchestrator plug-in works with vCenter Orchestrator 5.5.1 and 5.5.2.

For information about setting up Orchestrator, see *Installing and Configuring VMware vCenter Orchestrator*, available from the documentation page at https://www.vmware.com/support/pubs/orchestrator_pubs.html.

vCloud Automation Center

You must have access to a vCloud Automation Center server. The Horizon vCenter Orchestrator plug-in works with vCloud Automation Center versions 6.0.1 and 6.1. The embedded vCenter Orchestrator server packaged with vCloud Automation Center versions 6.0.1 and 6.1 is compatible with this plug-in, or you can install the plug-in on an external vCenter Orchestrator server.

For information about setting up vCloud Automation Center, see *vCloud Automation Center Installation and Configuration*, available from the documentation page at https://www.vmware.com/support/pubs/vcac-pubs.html.

vCenter Server and vCenter Single Sign-On

Verify that you have access to a vCenter Server 5.5.b instance and that you are using vCenter™ Single Sign-On™ 2.0.

For information about setting up vCenter Server 5.5, see *vSphere Installation and Setup*, available from the documentation page at https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html.

Install or Upgrade the Horizon vCenter Orchestrator Plug-In

Installing or upgrading the plug-in involves downloading the latest installer file and using the vCenter Orchestrator Configuration UI to upload the plug-in file and install the plug-in.

This topic provides specific guidance for installing the Horizon vCenter Orchestrator plug-in. The procedure for installing vCenter Orchestrator plug-ins is similar for all plug-ins, and the documentation for general plug-in installation, update, and troubleshooting is provided elsewhere. See the vCenter Orchestrator Documentation page at https://www.vmware.com/support/pubs/orchestrator_pubs.html.

Prerequisites

- Verify that you have the URL for downloading the Horizon vCenter Orchestrator plug-in installation file (`.vmoapp` file).
- Verify that you have vCenter Orchestrator (either the virtual appliance or the Windows service) set up and configured to work with vCenter Single Sign-On. See "Register Orchestrator as a vCenter Single Sign On Solution in Advanced Mode" in *Installing and Configuring VMware vCenter Orchestrator*.
- Verify that you have credentials for an account with permission to install vCenter Orchestrator plug-ins and to authenticate through vCenter Single Sign-On.
- Verify that you have installed VMware vCenter Orchestrator Client and that you can log in with Administrator credentials.

Procedure

1 Download the plug-in file to a location accessible from the vCenter Orchestrator appliance or service.

  The installer filename is `o11nplugin-horizon-1.1.0-xxxxxxx.vmoapp`, where *xxxxxx* is the build number.

2 Open a browser and launch the vCenter Orchestrator Configuration interface.

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

3 Click the **Plug-ins** item in the left pane and scroll down to the **Install new plug-in** section.

4 In the **Plug-in file** text box, browse to the plug-in installer file and click **Upload and install**.

  The file must be in `.vmoapp` format.

5 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: `Horizon (1.1.0 build xxxxxxx) Plug-in with same name was already installed (1.0.0 build xxxxxxx): overwriting existing plug-in.`

6 Go to the **Enabled plug-ins installation status** section and confirm that `Horizon 1.1.0.xxxxxxx` is listed, where *xxxxxx* is the build number.

You see a status message 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.`

7 Restart the vCenter Orchestrator Server service.

8 Restart the vCenter Orchestrator Configuration service.

9 Launch the vCenter Orchestrator Configuration interface again, click the **Plug-ins** item, and verify that the status changed to `Installation OK`.

What to do next

Launch the vCenter Orchestrator Client application, log in, and use the **Workflow** tab to navigate through the library to the `Horizon` folder. You can now browse through the workflows provided by the Horizon vCenter Orchestrator plug-in.

If you are upgrading, see "Post-Upgrade Configuration Tasks," on page 13.

Post-Upgrade Configuration Tasks

After upgrading to Horizon vCenter Orchestrator plug-in 1.1, you must perform some configuration tasks before running the newly added workflows.

1 Set access rights for delegated administrators on the newly created **GuestCredentialConfiguration** and **SelfServicePoolConfiguration** configuration elements in the `View` folder. See "Best Practices for Managing Workflow Permissions," on page 18.

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

Unmanaged machines are virtual machines that are managed by a vCenter instance that has not been added to View. That is, if you log in to View Administrator, and go to **View Configuration > Servers > vCenter Servers**, you will not see the vCenter Server instance in the list.

You must register an unmanaged machine with a View 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, to allow the specified delegated administrator to use the guest credentials and access the datacenter or virtual machine folder that contains the unmanaged virtual machine.

4 Run the Manage Self Service Pool Configuration workflow, in the `Configuration/Self Service Pool Configuration` folder, to specify which desktop and application pools will be available for self-service workflows in the newly added `Workflows/vCAC61` folder.

Configure the Connection to a View Pod

You run the Add View Pod workflow to provide the appropriate credentials for all workflow operations to be performed by the View Connection Server instance.

Prerequisites

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

Procedure

1 Log in to the Orchestrator client as an administrator.

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

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 View Connection Server instance is installed.

7 Provide the credentials of a user that has the View Administrators role.

8 Verify and accept the SSL certificate information.

9 Click **Submit** to run the workflow.

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

What to do next

Add a delegated administrator.

Updating View Pod Connection Information

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

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

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

Assigning Delegated Administrators to Desktop and Application Pools

The administrator runs a workflow to delegate responsibilities to delegated administrators. If your setup does not already contain a user group that has permission to register and update vCenter extensions, as well as permission to execute workflows in 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 Using vSphere Web Client on page 15

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

2 Provide Access Rights to the Horizon vCenter Orchestrator Plug-In Workflows on page 16

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

3 Assign Delegated Administrators to Pools on page 17

The administrator runs the Delegated Administrator Configuration workflow to set the scope of delegated administration. 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 Orchestrator.

Create a Delegated Administrator Role Using vSphere Web Client

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

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

Prerequisites

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

Procedure

1 Log in to the vSphere Web Client as administrator@vsphere.local or as another user with 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 you just 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 View Connection Server instance.

4 Create a role that has permission to read vCenter 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, you see that 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 you just created to the new group you created.

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

   b Select the appropriate vCenter 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, along with the role you just assigned.

What to do next

Provide the Delegated Administrators group access to the Horizon vCenter Orchestrator plug-in workflows. See "Provide Access Rights to the Horizon vCenter Orchestrator Plug-In Workflows," on page 16.

Provide Access Rights to the Horizon vCenter Orchestrator Plug-In Workflows

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

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

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter 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. See "Create a Delegated Administrator Role Using vSphere Web Client," on page 15.

Procedure

1 Log in to the Orchestrator client 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 is added to the list in the Edit Access Rights dialog box.

6 Click **Save and close**.

The group is added 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 is added 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," on page 17.

Assign Delegated Administrators to Pools

The administrator runs the Delegated Administrator Configuration workflow to set the scope of delegated administration. 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 Delegated Administrator Configuration workflow is required for configuring the Horizon vCenter Orchestrator plug-in because, 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 leveraged.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter 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 execute workflows for the Horizon vCenter Orchestrator plug-in. See "Provide Access Rights to the Horizon vCenter Orchestrator Plug-In Workflows," on page 16.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.

Procedure

1 Log in to the Orchestrator client as an administrator.

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

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 **Add Delegated Administrator Configuration** workflow and select **Start workflow**.

5 Complete the form that appears.

Option	Action
Horizon View Pod	Select the pod from the drop-down list. 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 list.
Select Application Pool IDs	Click **Not Set** and add one or more pools from the **New value** drop-down list.
Delegated Administrator User Name	Click **Not Set** and, in the **Filter** text box, type the name of the user you included in the delegated administrators group.

6 Click **Submit** to run the workflow.

The delegated administrator user you selected is now allowed to manage the desktop and application pools you specified in the form.

Best Practices for Managing Workflow Permissions

You can use the Orchestrator client to limit which personas can see and interact with the workflows. Ideally, only the administrator interacts with workflows in vCenter Orchestrator by using the Orchestrator client. Delegated administrators and end users should interact with the workflows through the vSphere Web Client or through the service catalog in vCloud Automation Center.

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

Important The suggested permission settings listed in this topic are required only if you want to hide the `CoreModules` folder and the configuration elements inside 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 therefore cannot even see the folders. This restriction will override 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 `vCAC60` folder and 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 vCenter Orchestrator documentation, available from the VMware vCenter Orchestrator Documentation page at https://www.vmware.com/support/pubs/orchestrator_pubs.html.

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 the **viewPodConfiguration**, **DA-configuration**, and **PoolPolicyConfiguration** configuration elements in the `View` folder, set the access rights so that delegated administrators have only View permissions.
- If you have Horizon vCenter Orchestrator plug-in 1.1, also set the access rights on the **GuestCredentialConfiguration** and **SelfServicePoolConfiguration** configuration elements in the `View` folder 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 vCenter Orchestrator documentation, available from the VMware vCenter Orchestrator Documentation page at https://www.vmware.com/support/pubs/orchestrator_pubs.html.

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 choose whether to actually delete the virtual machine and can choose 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 have several options:

- You can delete the virtual machine or you can simply unassign and unentitle the user.
- If you choose to delete the virtual machine and the virtual machine has a View Composer persistent disk, you can save the disk or delete it too.
- If you choose to save View Composer persistent disks, you can save them on their current datastore or save them to a different datastore.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Configure the connection to the View pod.
- Determine what you would like the policy to be regarding deleting the virtual machines and saving persistent disks. For information about persistent disks, see the topics about managing View Composer persistent disks in the *View Administration* document.

  If you choose to delete the virtual machine, you must choose whether to save any persistent disks. If you choose to save the disk to a different datastore, verify that you have the name of the datastore and the path to the folder that will store the persistent disk.

Procedure

1. Log in to the Orchestrator client as an administrator.
2. Click the **Workflows** view in the Orchestrator client.
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. Complete the form that appears and click **Submit**.

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

What to do next

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

Using Horizon vCenter Orchestrator Plug-In Workflows

3

You can use the predefined workflows installed by the Horizon vCenter Orchestrator plug-in, or you can copy workflows and customize them.

Important For security reasons, configuration workflows can be run only from within the Orchestrator client.

The folders and workflows that appear in the `Horizon` folder are the predefined workflows delivered by the Horizon vCenter Orchestrator plug-in. 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 different access rights that you can have when you work with the Orchestrator server depending on the type of license, vCenter Server see *Installing and Configuring VMware vCenter Orchestrator*.

This chapter includes the following topics:

- "Access the Horizon vCenter Orchestrator Plug-In Workflow Library," on page 21
- "Horizon vCenter Orchestrator Plug-In Workflow Library," on page 22
- "Horizon vCenter Orchestrator Plug-In Workflow Reference," on page 22
- "Syntax for Specifying User Accounts in the Workflows," on page 30

Access the Horizon vCenter Orchestrator Plug-In Workflow Library

You must use the Orchestrator client or the vSphere Web Client to access the elements from the Horizon vCenter Orchestrator plug-in workflow library.

Prerequisites

- Configure the connection to the View pod. See "Configure the Connection to a View Pod," on page 14
- Verify that you have credentials for logging in to the Orchestrator client as a user who can run Horizon vCenter Orchestrator plug-in workflows.

Procedure

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

Horizon vCenter Orchestrator Plug-In Workflow Library

The plug-in workflow library contains workflows that you can use to run automated processes to manage View pods, including objects such as remote desktops and applications, pools, entitlements, and View server configuration.

The folders and workflows provided by the Horizon vCenter Orchestrator plug-in are all created in the `Horizon` folder and are organized into various subfolders according to purpose and functionality. You can modify this folder structure without impacting the execution of the workflows.

Caution Some of the folders contain workflows that other workflows depend on. Do not modify these workflows.

Table 3-1. Folders Included with the Horizon vCenter Orchestrator Plug-In

Folder Name	Description
`Horizon`	Root folder for the Horizon vCenter Orchestrator plug-in.
`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. Configuration workflows should be executed only by administrators, from within the vCenter Orchestrator client.
`Configuration/Workflow Delegation`	Workflows an administrator can use to test whether a particular delegated administrator can successfully run the workflow. Some workflows might run in vSphere Web Client but not display a permissions error if the delegated administrator does not have the correct permissions.
`Workflows/Example`	Workflows that you can use as a basis to create customized workflows. **Note** Only the primary administrator will be able to run the Add Pool Policy in Batch workflow if you set the workflow permissions as recommended in this document.
`Workflows/vCAC60` `Workflows/vCAC61`	Workflows an administrator uses to create catalog items from within vCloud Automation Center. Some of the workflows in this folder are self-service workflows, which are designed to be used by end users for self-service access to virtual desktops and remote applications. These workflows are intended to be run only in vCloud Automation Center. **Note** You must have Horizon vCenter Orchestrator plug-in 1.1 to use the workflows in the `vCAC61` folder.
`Workflows/vSphereWebClient`	Workflows that are intended to be run by administrators or delegated administrators in vSphere Web Client but can also be run in the Orchestrator client.

Horizon vCenter Orchestrator Plug-In Workflow Reference

Each workflow has a specific purpose and requires certain inputs.

For the workflows in the `vCAC60` folder, the administrator must bind the workflow to a pod and pool. See "Bind vSphereWebClient Workflows to Specific Pods and Pools in vCenter Orchestrator," on page 32. When a delegated administrator or end user runs the workflow, the workflow operates only on the designated pod and pool.

Add Managed Machines to Pool

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Allows a delegated administrator to add vCenter-managed machines to a manual desktop pool in View. Here, the vCenter instance that manages the machines has been added to View. For example, if you look in View Administrator, you can go to **View Configuration > Servers > vCenter Servers**, and find the instance in the list.
Inputs/parameters	Pod, pool ID, list of virtual machines
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod.
Results	The selected virtual machines are added to a manual desktop pool.

Add Unmanaged Machines to Pool

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Allows a delegated administrator to add unmanaged virtual machines to a manual desktop pool in View. The unmanaged machines are in fact managed by a vCenter instance, but the vCenter instance has not been added to View. **Note** This workflow is not for adding physical machines or non-vSphere virtual machines. To add those types of machines, see "Adding Physical Machines and Non-vSphere Virtual Machines to Pools," on page 44.
Inputs/parameters	Pod, pool ID, list of virtual machines, guest credentials (see the Limitations row of this table)
Prerequisites	See "Prerequisites for Adding Unmanaged Machines to Pools," on page 43.
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool, pod, and guest credentials.
Results	The selected virtual machines are registered and added to a manual desktop pool. If you attempt to add multiple machines by using this workflow but some of the machines are not added for some reason, the workflow will fail and error messages will be included in the log file, specifying why those machines were not added. Other machines will be added successfully.
Limitations	■ If you want to add a machine back to an unmanaged pool that you previously removed from the pool in View, you must wait for some time before adding the machine back to the pool. ■ Choose virtual machines only from vCenter Server instances that have not been added to View. All vCenter Server instances are listed, meaning that vCenter Server instances that have been added to View are not filtered out. ■ If all virtual machines from the vCenter Server instance are not getting displayed in the virtual machine folder, you can choose machines from individual host folders. This issue can occur when the number of virtual machines is very large. ■ After you run the Add Guest Credentials workflow and the Manage Delegated Administrator Configuration for Registration workflow, it can take some time for the guest credentials to be populated in the vCloud Automation Center 6.1 service catalog. You might also need to log out of vCloud Automation Center 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 old guest credentials in the drop-down menu in the workflow. If you select these credentials and run the workflow, you get the error message: `Can not find credential named TestCredentials Dynamic Script Module name :getGuestCredential#7)`

Add User(s) to App Pool

Purpose	Allows a delegated administrator to entitle users to an application pool.
Inputs/parameters	Pod, pool ID, user names

Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required. If you do bind the workflow to a pod, in vSphere Web Client, you see a drop-down list of pools and the users entitled to each pool.
Results	Entitled users get direct access to specified applications.

Add User(s) to App Pools

Purpose	Allows a delegated administrator to entitle users to multiple application pools.
Inputs/parameters	Pod, pool IDs, user names
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to pools and a pod. For the `vSphereWebClient` folder, the administrator must bind this workflow to a pod. In vSphere Web Client, you see a drop-down list of pools and the users entitled to each pool.
Results	Entitled users get direct access to the specified application.

Add User(s) to Desktop Pool

Purpose	Allows a delegated administrator to entitle users to a desktop pool.
Inputs/parameters	Pod, pool ID, user names
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required. If you do bind the workflow to a pod, in vSphere Web Client, you see a drop-down list of pools and the users entitled to each pool.
Results	Users get entitled to the specified desktop pool. They can get a machine for floating pools or automatically assigned dedicated pools (subjected to availability). For other type of pools, users need to be assigned to the machine explicitly through the assignment workflows.

Application Entitlement

Purpose	Allows a delegated administrator to entitle users to an application pool and to remove users' entitlements.
Inputs/parameters	Pod, pool ID, users to entitle, and users to unentitle (selected from a default list)
Binding requirements	For the `vCAC60` and `vSphereWebClient` folders, the administrator must bind this workflow to a pool and pod.
Results	Entitlements can be added and removed in the same workflow.

Assign User

Purpose	Assigns a user to a specific machine in a desktop pool. An option is provided to entitle the user to a desktop pool as well.
Inputs/parameters	Pod, pool ID, machine name, user name
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
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

Purpose	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, user name

Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
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 the administrator specifies.

Desktop Allocation for Users

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Entitles multiple users to desktops in floating-assignment pools or RDS desktop pools. Entitles and assigns multiple users to machines for dedicated assignment pools (depending on availability). New machines are provisioned for users if the pool type is "specified naming."
Inputs/parameters	Pod, pool ID, user names, machine names (for specified naming pool)
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod.
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 others will not be 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, instead of adding a new line, the workflow is submitted.

Desktop Assignment

Purpose	Allows a delegated administrator to assign a user to a specific virtual machine and, optionally, entitle the user to the machine, and allows a delegated administrator to also remove an assignment for a user from a specific virtual machine, all in the same workflow.
Inputs/parameters	Pod, pool ID, machine name, user to assign, user to unassign
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
Results	Desktop assignments can be added and removed in the same workflow.

Desktop Entitlement

Purpose	Allows a delegated administrator to entitle users to a desktop pool and to remove users' entitlements.
Inputs/parameters	Pod, pool ID, users to entitle, and users to unentitle (selected from a default list)
Binding requirements	For the `vCAC60` and `vSphereWebClient` folders, the administrator must bind this workflow to a pool and pod.
Results	Entitlements can be added and removed in the same workflow.

Desktop Recycle

Purpose	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, user name
Scope	Works for all types of pools.
Prerequisites	Run the Add Pool Policy Configuration workflow before running this workflow.
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required. If you do bind the workflow to a pod, in vSphere Web Client, you see a drop-down list of pools and the users entitled to each pool.
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. For full-clone pools, if the virtual machine is deleted, the persistent disk is also deleted.
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.

Desktop Refresh

Purpose	Reverts a specific virtual machine to its base state.
Inputs/parameters	Pod, pool ID, machine name
Scope	Works only on automated View Composer linked-clone pools.
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
Results	For View Composer linked-clone virtual machines, a warning message is sent to the user if there is an active session, and the user is automatically logged out after a certain amount of time. A refresh operation then starts.

Register Machines to Pool

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Registers the supplied machine DNS names with a manual pool of unmanaged desktops in View. Use this workflow only for physical machines and non-vSphere virtual machines. **Note** As an alternative to running this workflow, you can use the Add Physical Machines to Pool workflow, available 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," on page 48. 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," on page 45 and "Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines," on page 47. You must also satisfy the prerequisites listed in "Prerequisites for Adding Unmanaged Machines to Pools," on page 43.
Inputs/parameters	Pod, pool ID, machine DNS names, guest OS
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod.

Results	Provided machine names are registered with the specified unmanaged desktop pool in View.
Limitations	■ This workflow registers any of the DNS names that are provided without performing any kind of 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, instead of adding a new line, the workflow is submitted. ■ To register a Windows Server 2008 R2 machine, you must first log in to View Administrator, select **View Configuration > Global Settings > General**, click **Edit**, and select the **Enable Windows Server 2008 R2 desktops** check box.

Remove Users from Application Pool

Purpose	Removes multiple users' entitlements from an application pool.
Inputs/parameters	Pod, pool ID, users (selected from a default list)
Binding requirements	For the `vCAC60` and `vSphereWebClient` folders, the administrator must bind this workflow to a pool and pod.
Results	Specified users are no longer entitled to the specified application pool.

Remove Users from Desktop Pool

Purpose	Removes multiple users' entitlements from a desktop pool.
Inputs/parameters	Pod, pool ID, users (selected from a default list)
Binding requirements	For the `vCAC60` and `vSphereWebClient` folders, the administrator must bind this workflow to a pool and pod.
Results	Specified users are no longer entitled to the specified desktop pool.

Self-Service Desktop Allocation

Purpose	Allows end users to allocate a machine to themselves. A new machine gets provisioned only for "specified naming" desktop pools.
Inputs/parameters	None
Scope	Works only on automated pools.
Prerequisites/binding requirements	■ For the `vCAC61` folder, the administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. ■ For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. 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 is provisioned for the user with the name the administrator specifies.

Self-Service Desktop Recycle

Purpose	Allows end users to de-provision their own virtual machine from the specified pod and desktop pool. This workflow removes user entitlement and assignment. 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 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.
Prerequisites/binding requirements	■ For the `vCAC61` folder, the administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. ■ For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. This workflow does not appear in the `vSphereWebClient` folder.
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. For full-clone pools, if the virtual machine is deleted, the persistent disk is also deleted.

Self-Service Desktop Refresh

Purpose	Reverts end user's virtual machine in the specified desktop pool to a base state.
Inputs/parameters	None
Scope	Works only on automated dedicated View Composer linked-clone pools.
Prerequisites/binding requirements	■ For the `vCAC61` folder, the administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. ■ For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. This workflow does not appear in the `vSphereWebClient` folder.
Results	For View Composer linked-clone virtual machines, a warning message is sent to the user if there is an active session, and the user is automatically logged out after a certain amount of time. A refresh operation then starts.

Self-Service Release Application

Purpose	Allows end users to remove their entitlement from the specified application pool.
Inputs/parameters	None
Prerequisites/binding requirements	■ For the `vCAC61` folder, the administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. ■ For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. This workflow does not appear in the `vSphereWebClient` folder.

Self-Service Request Application

Purpose	Allows end users to request an application for their own use. The user gets entitled to the specified application pool.
Inputs/parameters	None
Prerequisites/binding requirements	■ For the `vCAC61` folder, the administrator must run the Manage Self Service Pool Configuration workflow to specify which pools are available for selection by end users. ■ For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. This workflow does not appear in the `vSphereWebClient` folder.

Session Management

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Allows delegated administrators to disconnect, log off, reset, and send messages to active Horizon desktop sessions. Delegated administrators can perform these operations on user sessions as well.
Inputs/parameters	Pod, pool ID, operation, message (for the Send Message operation), user name, and other options

Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod.
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 and manual unmanaged desktop pools. ■ Multiple session selection is not supported when this workflow is executed from vSphere Web Client or the Orchestrator client. ■ The predefined list of users is not displayed when this workflow is executed from vCloud Automation Center 6.0.

Set Maintenance Mode

Purpose	(Available with Horizon vCenter Orchestrator plug-in 1.1) Allows a delegated administrator to put machines in maintenance mode and remove machines from maintenance mode.
Inputs/parameters	Pod, pool ID, operation, virtual machine
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod.
Results	The selected machines are "entered into maintenance mode" or "exited from maintenance mode."
Limitations	This workflow is not supported for RDS pools and manual unmanaged desktop pools.

Unassign User

Purpose	Removes the assignment of a user from a virtual machine.
Inputs/parameters	Pod, pool ID, machine name (as displayed in the View Administrator UI
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
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

Purpose	Changes the display name of an application pool.
Inputs/parameters	Pod, pool ID, new display name for pool
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
Results	The display name is changed, but the pool ID remains the same.

Update Desktop Pool Display Name

Purpose	Changes the display name of a desktop pool.
Inputs/parameters	Pod, pool ID, new display name for pool
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
Results	The display name is changed, but the pool ID remains the same.

Update Desktop Pool Min Size

Purpose	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, number to use for the minimum pool size (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.
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.

Update Desktop Pool Spare Size

Purpose	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, number of spare machines to have ready (an integer)
Binding requirements	For the `vCAC60` folder, the administrator must bind this workflow to a pool and pod. For the `vSphereWebClient` folder, no binding is required.
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 used for specifying users in the Horizon vCenter Orchestrator plug-in workflows is consistent across all workflows.

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

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

Important Non-ASCII characters are not supported.

Making the Workflows Available in vSphere Web Client and vCloud Automation Center

4

Administrators can expose the View workflows in the vCloud Automation Center self-service catalog or in the vSphere Web Client. Administrators can also bind the workflows to specific pools so that delegated administrators can select a pool and select entitled end users from a drop-down list.

Before end users and delegated administrators run workflows within vCloud Automation Center, you must specify which pools the workflows act on. For some workflows that delegated administrators run within vSphere Web Client, you must specify which pod or pools the workflows act on.

This chapter includes the following topics:

- "Exposing Horizon vCenter Orchestrator Plug-In Workflows in vSphere Web Client," on page 32
- "Exposing Horizon vCenter Orchestrator Plug-In Workflows in vCloud Automation Center," on page 34

Exposing Horizon vCenter Orchestrator Plug-In Workflows in vSphere Web Client

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

Bind vSphereWebClient Workflows to Specific Pods and Pools in vCenter 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 them to different pools as needed.

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

Important 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 list of pools:

- Application Entitlement
- Assign User
- Desktop Assignment
- Desktop Entitlement
- Unassign User

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.
- 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," on page 17.

Procedure

1. Log in to the 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 User(s) to Desktop Pool workflow in **Library > Horizon > Workflows > vSphereWebClient**.
3. Right-click the workflow, select **Duplicate Workflow**, and complete the form.

   The new workflow is placed in the folder 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 type in the same pod name enclosed with quotation marks.

   If you do not delete the **Predefined answers** property and set the **Default value** property, you might see a drop-down list 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, type the pool ID and enclose it with 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 with quotation marks.

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

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, located in the Configuration folder.

Prerequisites

- Bind the workflow to a pod and, optionally, to a pool. See "Bind vSphereWebClient Workflows to Specific Pods and Pools in vCenter Orchestrator," on page 32.
- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.

Procedure

1 Log in to the 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 exactly 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 Complete the form that appears.

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 Click **Submit** to run the workflow.

If the workflow completes successfully, you can go to the **Resources** view, expand the folder you created, and see the properties files that were created for each language.

Exposing Horizon vCenter Orchestrator Plug-In Workflows in vCloud Automation Center

vCloud Automation Center provides a service catalog with a request and approval engine that allows fine-grained control of workflows through entitlement and auditing. The workflows contained in the `vCAC60` folder in Orchestrator were created to work through vCloud Automation Center. These workflows require the administrator to configure them before exposing them to delegated administrators and end users.

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

1 Create Business Groups for Delegated Administrators and End Users on page 35

In vCloud Automation Center, users must belong to a business group before they can be entitled to a service created for a View plug-in workflow.

2 Create Services for Delegated Administrators and End Users on page 35

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

3 Create Entitlements for Delegated Administrators and End Users on page 36

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

4 Bind vCAC60 Workflows to Specific Pods and Pools in vCloud Automation Center on page 37

To expose a workflow through the vCloud Automation Center service catalog, the administrator must use vCloud Automation Center to bind the workflow to a specific pod and pool.

5 Bind vCAC61 Workflows to a vCAC User on page 38

One of the required parameters for the workflows in the `vCAC61` folder is vCAC User. You must configure that parameter to be requested by a principal ID.

6 Make vCAC61 Self-Service Workflows Use Specific Pools on page 40

You can run a workflow that limits which pools are available through the vCloud Automation Center Self-Service workflows.

7 Configure Output Parameters for vCAC61 Workflows on page 41

For workflows that return output parameters, you can add the output parameters to the service blueprint.

8 Configure the Catalog Item for the Workflow on page 42

In vCloud Automation Center, 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 vCloud Automation Center, users must belong to a business group before they can be entitled to a service created for a View plug-in workflow.

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

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Familiarize yourself with the procedures for creating groups in vCloud Automation Center. The vCloud Automation Center documentation is available at https://www.vmware.com/support/pubs/vcac-pubs.html.

Procedure

1 Log in to vCloud Automation Center as an administrator.

2 Click the **Infrastructure** tab.

3 Select **Groups > Fabric Groups** and create a fabric group with the administrator as a member.

4 Click **Business Groups** and 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 Click **OK** to add the new group.

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 Click **OK** to add the new group.

What to do next

Create corresponding services for delegated administrators and end users.

Create Services for Delegated Administrators and End Users

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

If you have been using vCloud Automation Center, you might have already created these services or equivalent ones.

Prerequisites

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

- Familiarize yourself with the procedures for creating services in vCloud Automation Center. The vCloud Automation Center documentation is available at https://www.vmware.com/support/pubs/vcac-pubs.html.

Procedure

1 Log in to vCloud Automation Center 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 Repeat the step to create a service for the end users business group.

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 vCloud Automation Center, administrators specify a business group and the service that corresponds to that group.

If you have been using vCloud Automation Center, you might have already created these entitlements or equivalent ones.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Create the business groups that contain the users you want to entitle. See "Create Business Groups for Delegated Administrators and End Users," on page 35.
- Create the services that correspond to the business groups you want to entitle. See "Create Services for Delegated Administrators and End Users," on page 35.
- Familiarize yourself with the procedures for creating entitlements in vCloud Automation Center. The vCloud Automation Center documentation is available at https://www.vmware.com/support/pubs/vcac-pubs.html.

Procedure

1 Log in to vCloud Automation Center 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, supply a name, and in the **Status** list, select **Active**.

   c From the **Business Group** list, select the business group that you just created for delegated administrators.

d In the **Users & Groups** field, 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 earlier.

f Click **Add**.

5 Repeat the step to create an entitlement for end users.

What to do next

Bind the Horizon vCenter Orchestrator plug-in workflows to pods and pools.

Bind vCAC60 Workflows to Specific Pods and Pools in vCloud Automation Center

To expose a workflow through the vCloud Automation Center service catalog, the administrator must use vCloud Automation Center to bind the workflow to a specific pod and pool.

Workflows exposed through vCloud Automation Center can be customized using the vCloud Automation Center form editor interface. You can hide fields or rearrange them and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize 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 list.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.
- Verify that vCloud Automation Center is configured to communicate with the vCenter Orchestrator server so that the vCenter Orchestrator workflows are available.
- Verify that you have the pod alias name and the pool IDs. You specified the pod alias when you performed the procedure described in "Configure the Connection to a View Pod," on page 14. The pool IDs are the desktop or application pool IDs, as shown in View Administrator.

Procedure

1 Log in to vCloud Automation Center as an administrator.

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

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

4 Navigate through the vCenter Orchestrator workflow library and select a workflow from the **Library > Horizon > Workflows > vCAC60** folder.

5 Click **Next**, and specify the workflow name and description that will appear in the vCloud Automation Center service catalog.

6 Click **Next**, and on the **Blueprint Form** tab, edit the **PodAlias** field.

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

b In the Edit Form Field - PodAlias dialog box, click the **Constraints** tab and configure the following fields.

Option	Action
Value	Select **Constant** and supply the pod alias that you configured when you ran the Add View Pod in Configuration workflow.
Visible	Verify that **No** is selected.

c Click **Submit**.

7 Edit the **PoolIds** field.

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

The Edit Form Field - PoolIds dialog box appears.

b On the **Details** tab, to create a drop-down list of pools, from the **Type** list, select **Drop-down**; otherwise, make no changes on this tab.

c Click the **Constraints** tab and configure the following fields.

Option	Action
Value	■ If you are binding this workflow to only one pool, select **Constant** and supply the pool ID, which is the pool ID shown in View Administrator. ■ If you are creating a drop-down list, select **Not Set**.
Visible	■ If you are binding this workflow to only one pool, verify that **No** is selected. ■ If you are creating a drop-down list, verify that **Yes** is selected.

d If you are creating a drop-down list, use the **Values** tab to add multiple pool IDs and display names.

e Click **Submit**.

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

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

The blueprint is added to the Service Blueprints page, and the status is set to Draft.

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

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

What to do next

Configure the catalog item for this service.

Bind vCAC61 Workflows to a vCAC User

One of the required parameters for the workflows in the vCAC61 folder is vCAC User. You must configure that parameter to be requested by a principal ID.

This procedure pertains only to the workflows that delegated administrators run. For the end-user self-service workflows in the vCAC61 folder, see "Make vCAC61 Self-Service Workflows Use Specific Pools," on page 40.

Workflows exposed through vCloud Automation Center can be customized using the vCloud Automation Center form editor interface. You can hide fields or rearrange them and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize 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 list.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.
- Verify that vCloud Automation Center is configured to communicate with the vCenter Orchestrator server so that the vCenter Orchestrator workflows are available.

Procedure

1 Log in to vCloud Automation Center as an administrator.

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

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

4 Navigate through the vCenter Orchestrator workflow library and select a workflow from the **Library > Horizon > Workflows > vCAC61** folder.

5 Click **Next**, and specify the workflow name and description that will appear in the vCloud Automation Center service catalog.

6 Click **Next**, and on the **Blueprint Form** tab, edit the **vCACUser** field.

   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 catalog request.

   h Click **Submit**.

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

   The blueprint is added to the Service Blueprints page, and the status is set to Draft.

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

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

What to do next

Configure the catalog item for this service.

Make vCAC61 Self-Service Workflows Use Specific Pools

You can run a workflow that limits which pools are available through the vCloud Automation Center Self-Service workflows.

This procedure pertains only to self-service workflows. For the other workflows in the vCAC61 folder, see "Bind vCAC61 Workflows to a vCAC User," on page 38.

Workflows exposed through vCloud Automation Center can be customized using the vCloud Automation Center form editor interface. You can hide fields or rearrange them and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize 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 list.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.
- Verify that vCloud Automation Center is configured to communicate with the vCenter Orchestrator server so that the vCenter Orchestrator workflows are available.

Procedure

1 Log in to the Orchestrator client as an administrator.

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

3 In the workflows hierarchical list, select **Library > Horizon > Configuration > Self Service Pool Configuration** and navigate to the **Manage Self Service Pool Configuration** workflow.

4 Right-click the **Manage Self Service Pool Configuration** workflow and select **Start workflow**.

5 Select the pod from the list, and click the appropriate radio button to specify whether to include all pools.

6 If you do not want to make all pools available, specify which pools to include:

   a Click in the fields for selecting specific pool IDs.

   b In the list of pools that appears, select a pool to exclude and click the red X button above the list.

   Repeat this step until you remove the pools that are not to be available. If you accidentally remove an item from the list, you can use the **New value** drop-down box to insert the pool in the list.

   c Use the arrow buttons to change the order in which pools are displayed.

   d Click **Accept**.

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

The specified desktop and application pools are available in the self-service workflows of the vCAC61 folder.

Configure Output Parameters for vCAC61 Workflows

For workflows that return output parameters, you can add the output parameters to the service blueprint.

Workflows exposed through vCloud Automation Center can be customized using the vCloud Automation Center form editor interface. You can hide fields or rearrange them and add cosmetic improvements to fit into the organization service catalog. Add the blueprint for the specific workflow and customize 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 list.

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that a connection has been made to the View pod by running the Add View Pod in Configuration workflow. See "Configure the Connection to a View Pod," on page 14.
- Verify that vCloud Automation Center is configured to communicate with the vCenter Orchestrator server so that the vCenter Orchestrator workflows are available.

Procedure

1 Log in to vCloud Automation Center as an administrator.

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

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

4 Navigate through the vCenter Orchestrator workflow library and select a workflow from the **Library > Horizon > Workflows > vCAC61** folder.

5 Click **Next**, and specify the workflow name and description that will appear in the vCloud Automation Center service catalog.

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

7 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**.

8 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 could click the **htmlAccessUrl** item under **Outputs** in the Fields list, and drag the **htmlAccessUrl** item onto the form page.

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

The blueprint is added to the Service Blueprints page, and the status is set to Draft.

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

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 using this catalog item, if you go to the **Requests** tab and view the details of one of the requests for this item, you see the output parameters listed on the **Step** tab.

Configure the Catalog Item for the Workflow

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

Prerequisites

- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Verify that you have published the workflow as a service blueprint. See "Bind vCAC60 Workflows to Specific Pods and Pools in vCloud Automation Center," on page 37 or "Bind vCAC61 Workflows to a vCAC User," on page 38.

Procedure

1 Log in to vCloud Automation Center as an administrator.

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

3 From the **Actions** list next to the item, select **Configure**.

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

The workflow is now ready to be run by the delegated administrator or end user. When the delegated administrator or end user logs in to vCloud Automation Center and goes to the **Catalog** tab, the service, or workflow, is listed. The user clicks the **Request** button, completes the form that appears, and clicks **Submit** to run the workflow.

To check the status of the request, the user can go to the **Request** tab.

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

Working with Unmanaged Machines 5

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

The topic "Prerequisites for Adding Unmanaged Machines to Pools," on page 43 applies to all types of unmanaged machines. The other topics in this chapter apply only to physical machines that you add to a View desktop pool.

Note The Add Unmanaged Machines to Pool workflow is available with Horizon vCenter Orchestrator plug-in 1.1.

This chapter includes the following topics:

- "Prerequisites for Adding Unmanaged Machines to Pools," on page 43
- "Adding Physical Machines and Non-vSphere Virtual Machines to Pools," on page 44

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 allow a delegated administrator to add physical and virtual machines to manual desktop pools in View. These workflows are available with Horizon vCenter Orchestrator plug-in 1.1.

- Use the Add Unmanaged Machines to Pool workflow for unmanaged machines that are in fact managed by a vCenter instance, but the vCenter instance has not been added to View.
- Use the Add Physical Machines to Pool workflow, available in the `Workflows/Example` folder, for adding physical machines and non-vSphere virtual machines, such as those you can create with Citrix XenServer, Microsoft HyperV, or VMware Workstation. Alternatively, you can run the other workflows as described in "Adding Physical Machines and Non-vSphere Virtual Machines to Pools," on page 44.

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

- 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 View Agent 6.0 or 6.0.1 in the unmanaged machine.

  For step-by-step instructions, see the topic "Install View Agent on an Unmanaged Machine," in *Setting Up Desktop and Application Pools in View* .

- If the unmanaged machine is a Windows Server 2008 R2 machine, enable the server to be used as a remote desktop:
  a Log in to View Administrator.

    The View Administrator interface uses a URL with the following format: https://*connection-server*/admin.

  b Go to **View Configuration > Global Settings**.

  c Select the **General** tab and click **Edit**.

  d Select the **Enable Windows Server 2008 R2 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:
  a Log in to the vCenter Orchestrator configuration console.

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

  b Go to **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 vCenter Orchestrator Server service.
- Add guest credentials by running the Add Guest Credentials workflow of the Horizon vCenter Orchestrator plug-in.

  This workflow is located 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.
- Run the Manage Delegated Administrator Configuration for Registration workflow, in the `Configuration/Horizon Registration Configuration` folder, to allow the delegated administrator to use the guest credentials and have access to the datacenter and virtual machine folders.

The Add Unmanaged Machines to Pool workflow, for vSphere virtual machines, has some important limitations. See "Add Unmanaged Machines to Pool," on page 23.

For physical machines and non-vSphere virtual machines, you must perform additional configuration tasks. See "Configure a Physical Machine for an Unmanaged Pool," on page 45 and "Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines," on page 47. You can then run the Add Physical Machines to Pool workflow, available in the `Workflows/Example` folder, or else run the Register Machines to Pool workflow and the PowerShell workflows mentioned in "Run Workflows to Add Physical Machines as PowerShell Hosts," on page 48.

Adding Physical Machines and Non-vSphere Virtual Machines to Pools

Several configuration tasks are required for adding physical machines and non-vSphere virtual machines, such as those you can create with Citrix XenServer, Microsoft HyperV, or VMware Workstation, to manual unmanaged desktop pools.

After you satisfy the requirements listed in "Prerequisites for Adding Unmanaged Machines to Pools," on page 43 you must complete the following tasks:

1 Enable Windows Remote Management, set remote execution policies, add the Orchestrator server as a trusted host, and enable communication with the PowerShell plug-in. For instructions, see "Configure a Physical Machine for an Unmanaged Pool," on page 45.

2 Configure the Orchestrator server to use Kerberos authentication. For instructions, see "Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines," on page 47.

3 Either run the Add Physical Machines to Pool workflow, available in the `Workflows/Example` folder, or else run the Register Machines to Pool workflow and run the PowerShell workflows described in "Run Workflows to Add Physical Machines as PowerShell Hosts," on page 48.

Configure a Physical Machine for an Unmanaged Pool

Before you add a physical machine to 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.
- Familiarize yourself with the procedure for configuring WinRM to use HTTP. See Configure WinRM to Use HTTP, in 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.

   For example, on Windows 7 machines, you can go to **Start > Administrative Tools > Services**.

   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 Launch 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 vCenter 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 will be similar to:

```
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 communication with the PowerShell plug-in through the HTTP protocol.

If you use PowerShell 2.0, be sure to 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 View Agent in the physical machine.

What to do next

Configure authentication on the vCenter Orchestrator server. See "Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines," on page 47.

Configure vCenter Orchestrator to Use Kerberos Authentication with Physical Machines

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

Prerequisites

You must have the root password if you are using the vCenter Orchestrator virtual appliance or the administrator credentials if vCenter Orchestrator is installed in a Windows server.

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 located in `etc/krb5.conf`, 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 Open the `krb5.conf` file with a text editor 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 needs to be registered) and the domain controller host names can be resolved from the vCenter Orchestrator server.

The DNS of the vCenter 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 vCenter Orchestrator server.

On a virtual appliance, this file is located at `/etc/hosts`.

7 Restart the vCenter Orchestrator Server service.

What to do next

Add physical machines as PowerShell hosts. See "Run Workflows to Add Physical Machines as PowerShell Hosts," on page 48.

Note As an alternative to running the PowerShell workflows, you can use the Add Physical Machines to Pool workflow, available 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," on page 48. Before you run the Add Physical Machines to Pool workflow, you must perform the tasks descrbed in "Configure a Physical Machine for an Unmanaged Pool," on page 45 and "Prerequisites for Adding Unmanaged Machines to Pools," on page 43.

Run Workflows to Add Physical Machines as PowerShell Hosts

You must run some PowerShell plug-in workflows to complete the process of adding physical machines and non-vSphere virtual machines to desktop pools using the Horizon vCenter Orchestrator 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, available in the `Workflows/Example` folder.

Prerequisites

- Verify that you have the vCenter Orchestrator Plug-In for Microsoft Windows PowerShell, which contains the workflows required for this procedure .
- Verify that you have administrator credentials for the Orchestrator server. The account must be a member of the vCenter Orchestrator Admin group configured to authenticate through vCenter Single Sign-On.
- Run the Register Machines to Pool workflow to register all machine DNS names into manual unmanaged desktop pools in View. The Register Machines to Pool workflow returns a token (one for each registered DNS) that will be pushed into the Windows Registry of the machines when you run the PowerShell command described in this procedure.

Procedure

1 Log in to the Orchestrator client as an administrator.

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

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 Complete the form that appears and click **Next**.

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

7 Complete the form that appears.

Option	Action
Session mode	Select **Shared session** from the drop-down list.
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 Click **Submit** to run the workflow.

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

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

11 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.

12 Click **Submit** to run the workflow.

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

Index

A

access rights **18**
access rights to the plug-in **16**
Add Delegated Administrator Configuration workflow **17**
Add Unmanaged Machines to Pool workflow, prerequisites **43**
Add View Pod workflow **14**
adding access rights **18**
architecture **9**

B

bind a workflow to a pod or pool **32, 37**
bind a workflow to a vCAC user **38**
business groups **35**

C

catalog services **35**
configure catalog items **42**
credentials, syntax for supplying **30**

D

de-provisioning desktop virtual machines **19**
delegated administrators **15**

E

editing access rights **18**
entitlements in vCloud Automation Center **36**

F

functions **8**

H

Horizon workflows **21**

I

installation **11, 12**
intended audience **5**

K

Kerberos authentication **47**

L

localization **33**

O

output parameters for vCAC61 workflows **41**

P

personas **10**
physical machines **44**
physical machines in pools **45**
Pool Policy Configuration workflow **19**
PowerShell plug-in **48**
privileges **10**

R

roles **10**

S

self-service **31**
system requirements **11**

T

trusted account security model **9**

U

unmanaged machines **43**
upgrade **12, 13**
using the plug-in **7**

V

vCenter extensions **15**
vCenter Orchestrator **8**
vCloud Automation Center **31, 34**
vCloud Automation Center catalog **40**
View pod **14**
vSphere Web Client **31, 32**

W

workflow descriptions **22**
workflow library **21, 22**
workflows, overview **8**