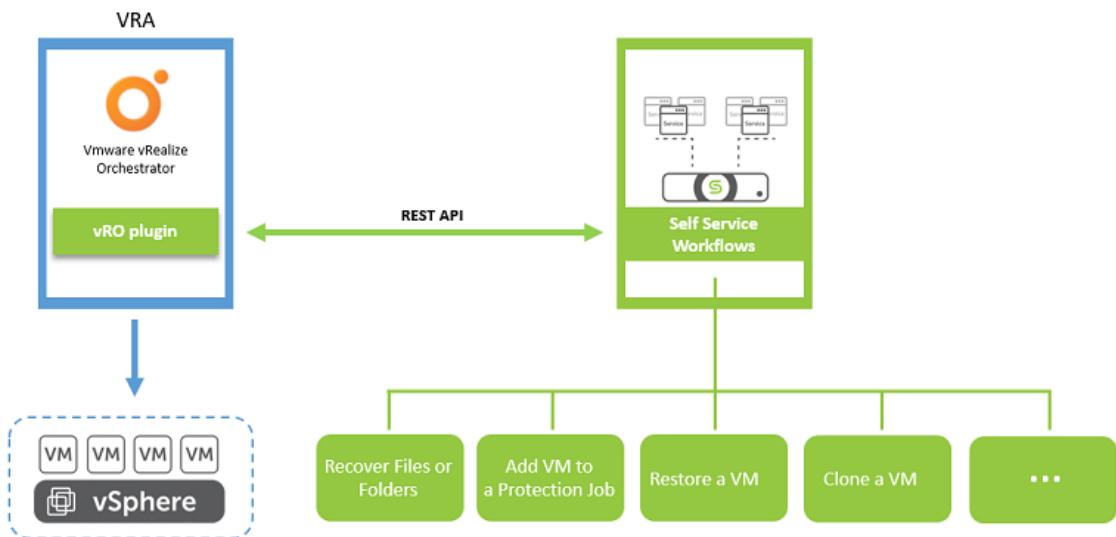


# Cohesity vRO Plugin Deployment Guide

The **Cohesity vRealize Orchestrator (vRO)** Plugin provides self-service workflows for **Cohesity DataPlatform**. The **vRO plugin** is developed on the **Vmware vRealize Orchestrator** component of the **VMware vRealize Automation**. This plugin uses REST APIs to interact with the **Cohesity DataPlatform**. Using this vRO plugin, you can execute many self service workflows such as Add VM to protection job, Restore a VM, Clone a VM and so on. See [Workflows](#) for details.

You can download the vRealize Orchestrator Plugins and workflows from [VMware Solution Exchange](#).



## vRO Self Service Workflows

The plugin provides a list of workflows that you can access on the **Workflows** tab of the Orchestrator client. The plugin contains packages of workflows and actions that you can run on the objects in the inventory to automate the typical use cases of the integrated product.

<b>Custom Objects</b>	<b>Workflows</b>	<b>Privileges</b>
Initial Configuration	Add a Cohesity Endpoint	
	Remove a Cohesity Endpoint	
	Update a Cohesity Endpoint	
	Add an Email Configuration	
	Remove an Email Configuration	
	Update an Email Configuration	
Day-1 Workflows	Add multiple VMs to Protection Job	
	Remove VM from all Protection Job	
Protection Job Workflows	Add Unprotected VM/Physical server to Protection Job	Read Cohesity Storage Domains
		View Protection Groups
		View Protection Policies
		Manage Protection Groups
	Add Protection Source	Manage Sources
	Delete Protection Group	Manage Protection Groups
		View Protection Policies
	Clone Virtual Machine	View Clone Tasks
		Manage Clone Tasks

Custom Objects	Workflows	Privileges
	Move VM to new Protection Source	Manage Protection Groups
		View Protection Groups
	Remove VM/Physical server from Protection Source	Manage Protection Groups
		View Protection Policies
	Remove VM Tag from Protection Job	Manage Protection Groups
		View Protection Policies
	Delete Protection Group	Delete Protection Group
	Restore Virtual Machine	View Protection Groups
		Manage Recover Tasks
		View Recover Tasks
	Run Protection Job on Demand	View Protection Groups
		Protection Group Operator
	Generate Reports	View Protection Groups
		Reporting
	Recover Files or Folders	View Protection Groups
		Manage Recover Tasks
		View Recover Tasks

## Features

The vRO plugin provides an inventory of objects that you can access on the Inventory tab of the Orchestrator client, along with packages of workflows and actions that you can run on these objects in the inventory to automate the typical use cases of the integrated product.

- **Managing Cohesity Data Operations:** Allows vRO user to perform operations for backups, data protection, restore and clone on Cohesity sources such as Virtual Machines and vCenters.
- **Managing Data with Multiple ESXi Boxes:** Move protected VM/data within protection groups and also clone and restore over different ESXi boxes.
- **Multiple Platform Support:** Management of multiple Cohesity DataPlatform setups.

## Software Requirements

Software	Version	Provider
vCenter Server	5.5 or later	VMware
vRealize Automation	7.x	VMware
Cohesity DataPlatform	6.x or later	Cohesity
Web browsers	Latest	Mozilla Firefox, Google Chrome

## vRA - Cohesity Compatibility Matrix

Plugin Release Version	vRA Version	Cohesity Cluster Version
v1.0.2, v1.0.4, v1.0.5, v1.0.6, v1.0.7, v2.0.1	7.5 or higher	6.3 or higher
v2.1.1	7.5 or higher	6.5, 6.4.1c

## Process Overview

A snapshot of the overall process involved in using the Cohesity vRO plugin is as follows:

1. [Install the Cohesity vRO Plugin](#)
2. [Configure the Cohesity Plugin](#)
  1. [Add Cohesity Endpoints](#) (Mandatory)
  2. [Add Email Configurations](#) (Optional)
3. [Configure vRA](#)
  1. [Importing Blueprints](#)
  2. [Configuring Day 1 Workflows](#)
4. [Execute Protection Group Workflows](#)

## What's New

Version	What's New	Revision Date
v2.1.2	Support for multi-tenancy workflows.	July 2020
v2.1.1	This release introduces the Recovery method in Recover Files or Folders workflow.	May 2020
v2.0.1	This release describes details about the vRA workflow privileges.	Apr 2020
v1.0.5	This release introduces new workflows to Remove VM Tag from Protection Group and to Generate Reports.	Nov 2019
v1.0.4	This release introduces the ability to upgrade the Cohesity agent on physical sources. This release also included minor bug fixes.	Oct 2019
v1.0.3	This release introduces new workflows to add/remove protection source, add/remove physical server to/from protection group and create/delete protection groups.	Aug 2019

Version	Second Draft of vRO plugin documentation. The document has <b>What's New</b> been updated with the current procedures to execute workflows.	Revision Date
v1.0.1	First draft released.	Nov 2018

# Installing the Cohesity vRO Plugin

## In This Section

Topic	Description
<a href="#">Installing the Plugin</a>	This section describes the detailed steps to install the Cohesity vRO plugin.
<a href="#">Removing the Plugin</a>	This section provides information on disabling and removing the Cohesity vRO plugin.

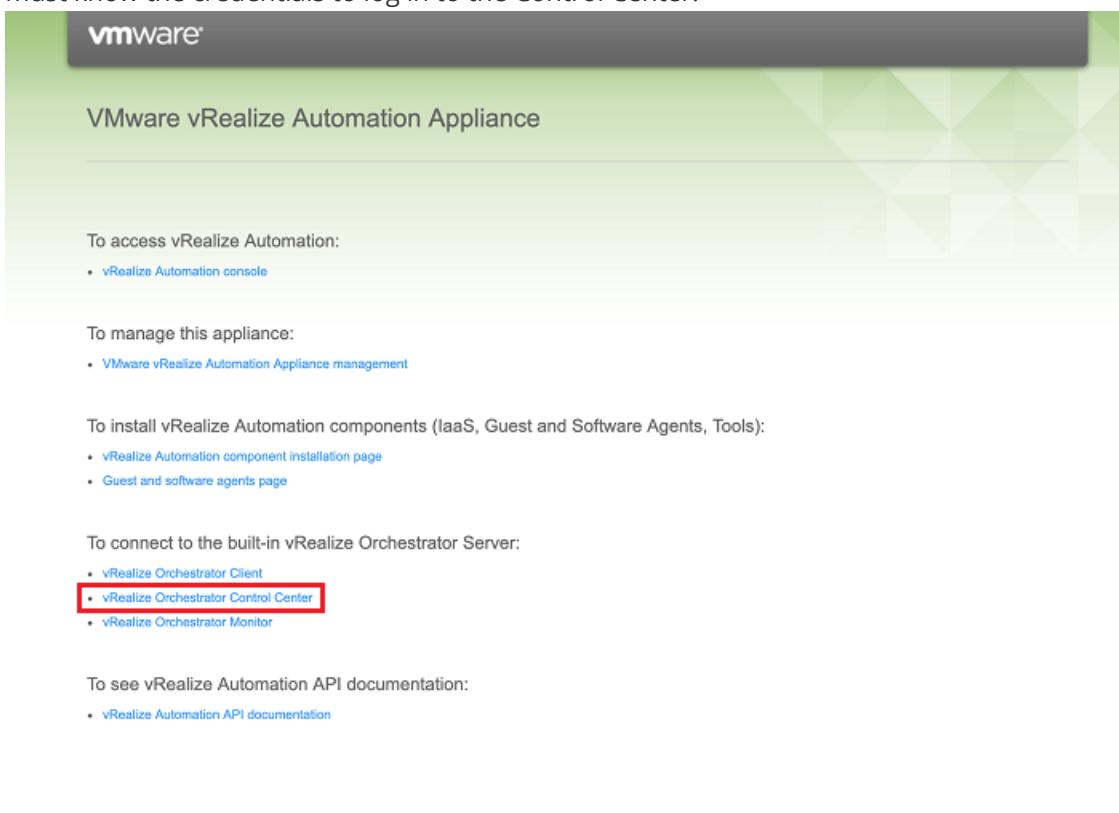
## Installing the Plugin

This section describes the detailed steps to install the Cohesity vRO plugin.

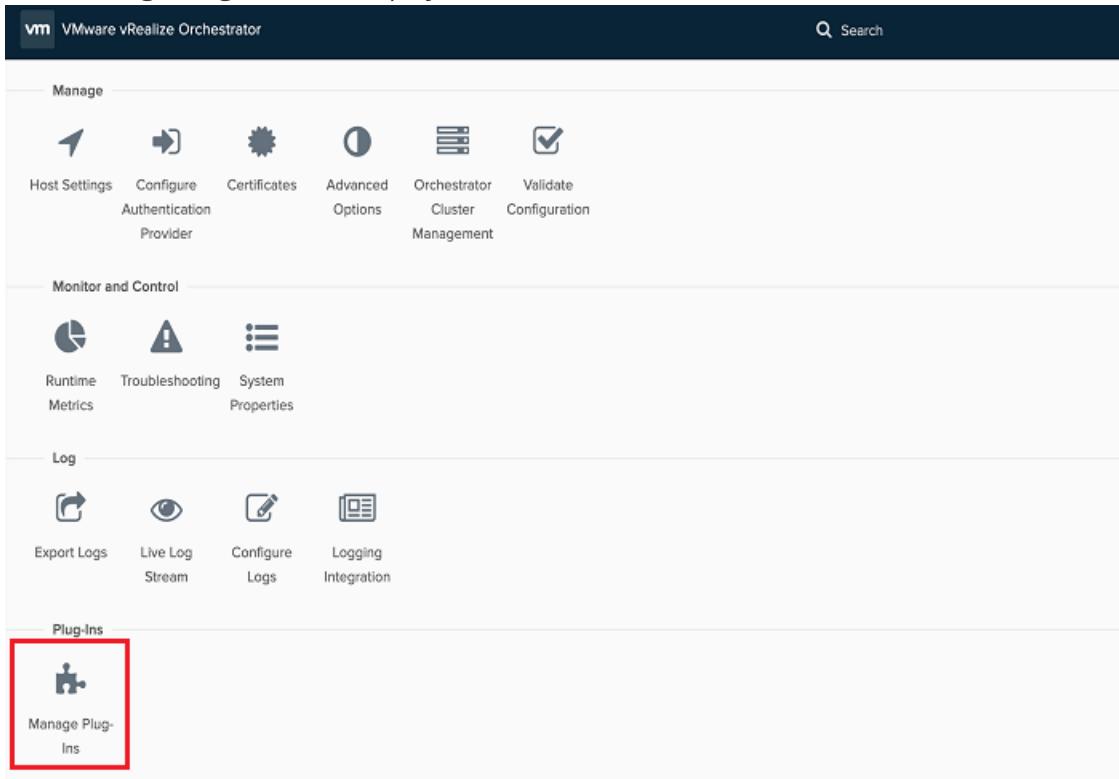
**Note:** If the Cohesity vRO plugin has already been installed and must be upgraded, you must first [remove](#) the existing plugin and then install the new Cohesity vRO plugin.

### Procedure

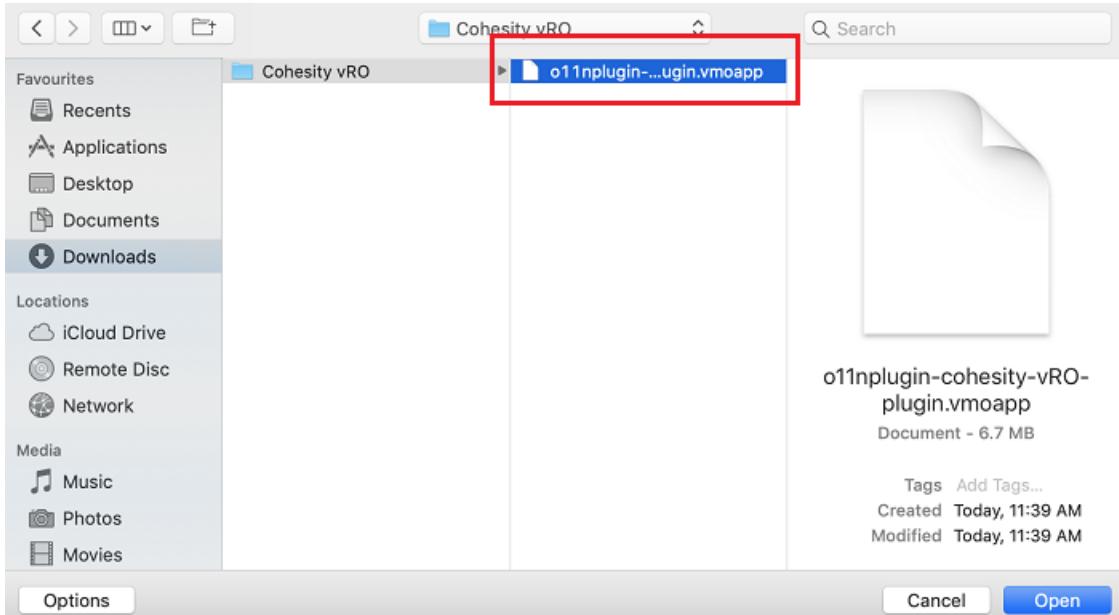
1. Login to the **vRealize Orchestrator** and click **vRealize Orchestrator Control Center**. You must know the credentials to log in to the Control Center.



2. Click **Manage Plugins** in the displayed **vCenter Control Center** window.



3. In the **Manage Plugins** section, click **Browse** to navigate to the folder where you have saved the **.vmoapp** file and select the source installer ***o11nplugin-cohesity-vRO-plugin.vmoapp/.dar***.



4. Click **Install**.

## 5. Read the end user license agreement and click **Accept EULA**.

The screenshot shows the 'Manage Plug-ins' interface with the 'Install plug-in' tab selected. It displays the Cohesity plugin for vRealize Orchestrator version 1.0.2.1559040312. The EULA text is present, and the 'Accept EULA' button is highlighted with a red box. Below the EULA, there are 'CANCEL' and 'INSTALL' buttons.

## 6. Click **INSTALL**. On successful installation of the plugin, the following screen is displayed.

The screenshot shows the 'Manage Plug-Ins' interface with the 'Plug-in(s) installed' section. It lists the 'Plug-in 'CS' (1.0.2 build 1559040312)' as installed. A note at the bottom states: 'The Orchestrator server service will restart 2 minutes after the last configuration change.'

## 7. Now you can open **vRO**. The plugin is added to the list. On selecting the plugin, the version and details of the plugin are displayed as follows:

The screenshot shows the 'Control Center' page of vRealize Orchestrator. The 'Manage Plugins' section lists the 'Cohesity plug-in for vRealize Orchestrator' with version 1.0.2.1559040312. The 'Logging level' dropdown is set to 'DEFAULT' and has a green toggle switch. A note at the top right says: 'Changes are made but not saved.'

# Removing the Plugin

## Procedure

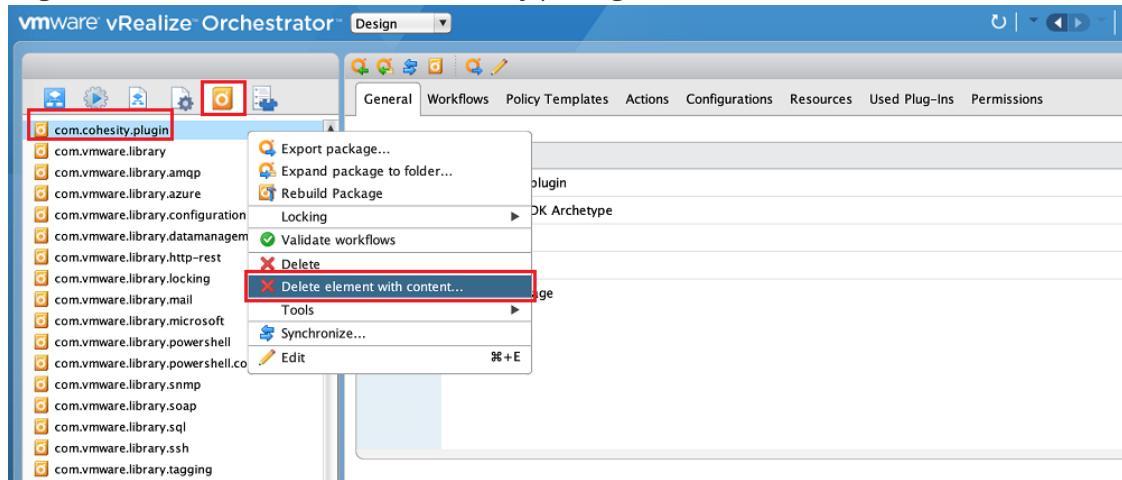
This section provides information on disabling and removing the vRO plugin.

1. In a supported browser, launch the **Control Center**. The VMware Orchestrator startup page is displayed.
2. Click the **Orchestrator Control Center** link. The **Control Center** page is displayed.
3. Click **Manage Plugin** in the Control Center. The **Manage Plugin** page is displayed.
4. Toggle off the Cohesity plugin to disable the plugin. Click **Save Changes**.

The screenshot shows the 'Manage Plugins' screen with the Cohesity plugin for vRealize Orchestrator disabled (green toggle switch). The 'SAVE CHANGES' button is highlighted with a red box. Other plugins like AD, AMQP, and Azure are also listed with their respective status and logging levels.

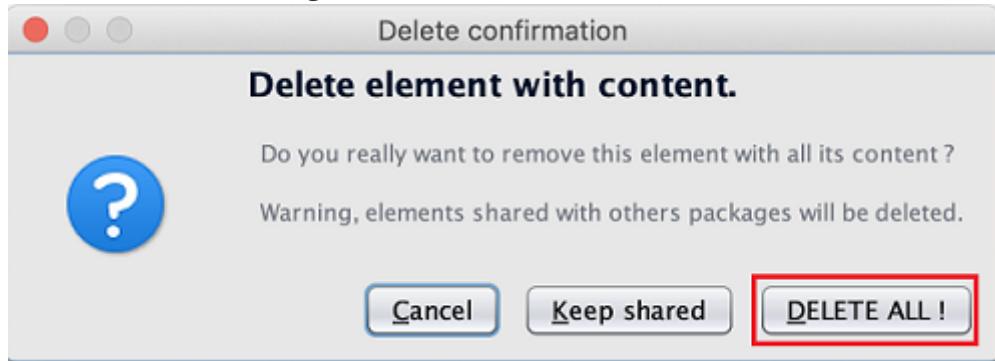
Alternatively, you can also click the **Remove** icon to remove the plugin.

5. Log in to vRO client and delete the Cohesity package.



**Note:** For details on removing the plugin from vRO, see [here](#).

6. In the confirmation dialog box, click **DELETE ALL**.



7. Restart the server. The plugin is disabled or removed accordingly.

## Getting Started with Cohesity vRO Plugin

This section provides the initial configuration, details to add a Cohesity endpoint and Email configuration.

### In This Section

Topic	Description
<a href="#">Launching vRO Client</a>	This section describes the basic steps to start the vRO Client.
<a href="#">Adding a Cohesity Endpoint</a>	This section describes the details to add an endpoint and to connect vRO with the Cohesity Data Platform
<a href="#">Adding an Email Configuration</a> (Optional)	This section describes the details about Email configuration to send notification to the intended recipients.

## Launching vRO Client

This section describes the basic steps to start the vRO client

### Prerequisites

Java (JDK version 7 or later) must be installed on the client side.

### Before You Start

1. Go to the home page of *vra-appliance-ip*.
2. Click on **vRealize Orchestrator** client.  
A *client.jnlp* file is downloaded.
3. Open command prompt and run the following command.

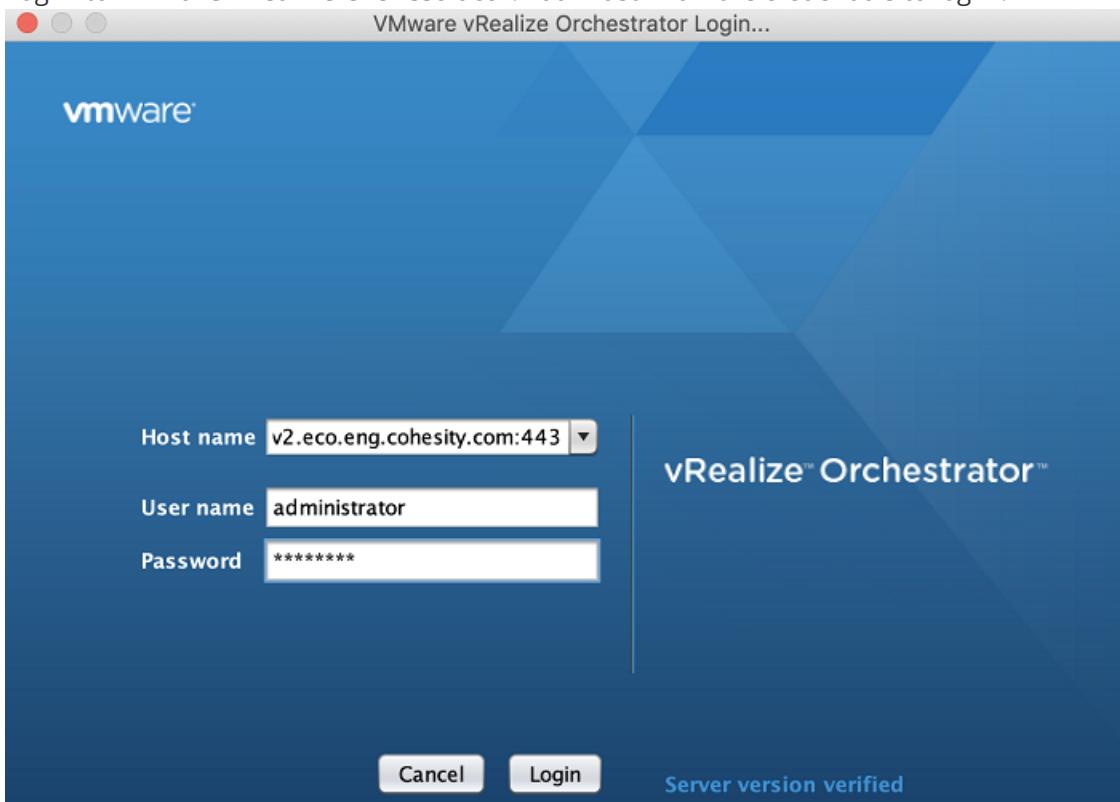
**javaws client.jnlp**

**Note :** The above mentioned steps are not mandatory to be executed if the VRA version is 7.5 or later. The client can directly access the HTML client interface available in VRA to configure the Cohesity plugin.

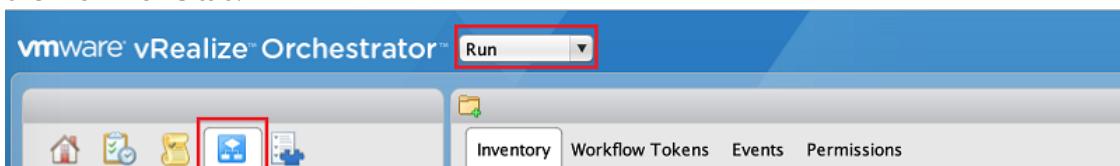
### Procedure

The following procedure is to log in to the vRO client.

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.



2. Select **Run** mode from the drop-down list located at the top left of the page and then click the **Workflows** tab.



3. Select **Library > Cohesity**. All the workflows are listed in the left pane.

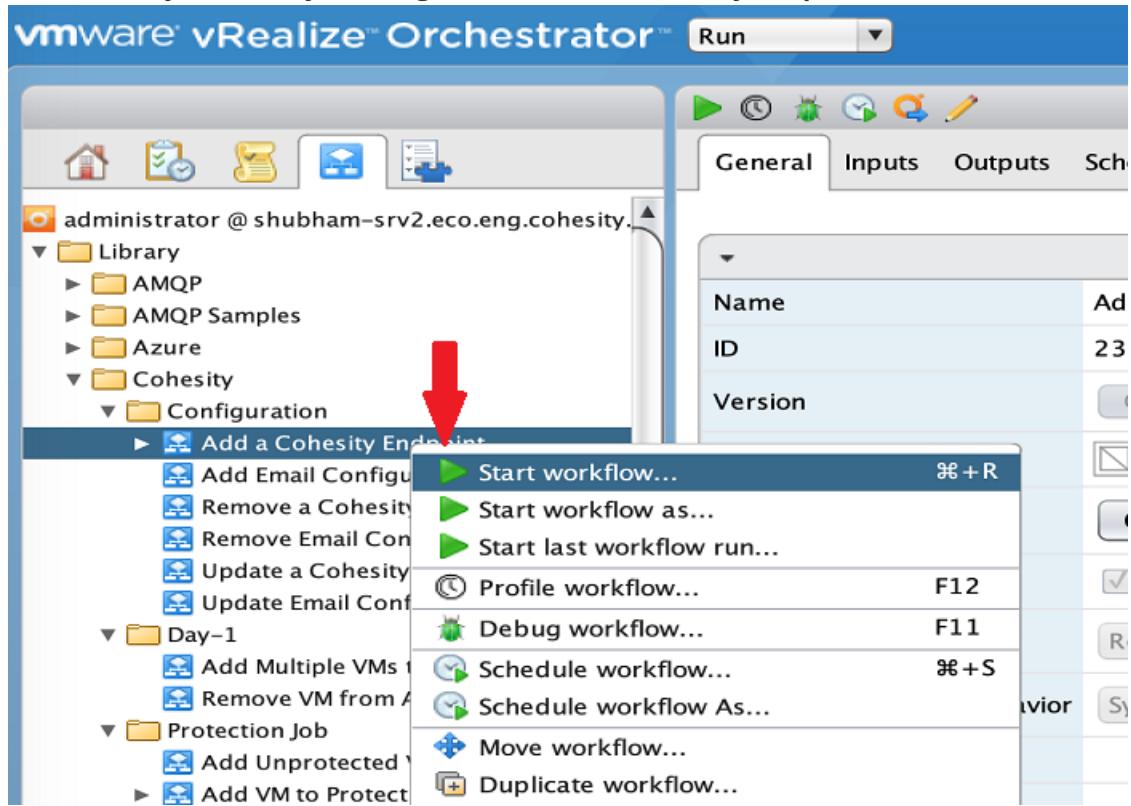
## Adding a Cohesity Endpoint

### Procedure

This section describes the details to add an endpoint and to connect vRO with the Cohesity data platform.

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the **Workflows** tab.

3. Select Library > Cohesity > Configuration > Add a Cohesity Endpoint.



4. To start the workflow, click or right click and select **Start workflow...**

The screenshot shows the 'Add Cohesity Endpoint' configuration window. At the top, there is a message: 'Start Workflow : Add a Cohesity Endpoint' with a play button icon. Below this, the title bar says 'Add Cohesity Endpoint' with a red error icon. A yellow box at the top indicates '2 errors - [Endpoint Name], Mandatory field not set'. The form contains five fields with red asterisks indicating they are mandatory:

- \* Endpoint Name: An empty input field.
- \* Hostname or IP address of Cohesity Cluster: An empty input field.
- \* Domain Name: An input field containing 'LOCAL'.
- \* User Name: An empty input field.
- \* Password: An empty input field.

At the bottom right are 'Cancel' and 'Submit' buttons.

The **Add a Cohesity Endpoint** window is displayed

5. Enter the following details:

- **Endpoint Name:** Enter an endpoint name.
- **Hostname or IP address of Cohesity Cluster:** Enter the Cohesity data platform URL you want to connect to.
- **Domain Name:** This is the user defined domain name.
- **User Name and Password:** Enter the credentials of the Cohesity DataPlatform.

6. Click **Submit** to add an endpoint successfully.

## Adding an Email Configuration

This section describes the details about Email configurations to send notification to the intended recipients for Recover of Files or Folders workflow.

### Procedure (Optional)

To add an Email configuration:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the **Workflows** tab.
3. Select **Library > Cohesity > Configuration > Add Email Configuration**.
4. To start the workflow, click . The **Add Email Configuration** screen is displayed.

The screenshot shows the 'Add Mail Basic Configuration' dialog box. The title bar displays 'Start Workflow : Add Email Configuration'. The main content area is titled 'Add Mail Basic Configuration'. It contains seven input fields, each preceded by a red asterisk indicating it is a required field:

- \* Email Configuration Name
- \* Email Server SMTP Host
- \* Email Server SMTP Port
- \* Email Server User Name
- \* Email Server Password
- \* From Email Id
- \* From Name

At the bottom right of the dialog are two buttons: 'Cancel' and 'Submit'.

5. Enter the following details:

- o **Email Configuration Name:** Enter an Email configuration name to identify while using it in another workflow.
- o **Email Server SMTP Host:** Enter the SMTP host name such as gmail.com
- o **Email Server SMTP Port:** Enter the SMTP port number.
- o **Email Server User Name:** Enter the Email server user name.
- o **Email Server Password:** Enter the Email server password.
- o **From Email Id:** Enter the Email ID from where the notification is sent.
- o **From Name:** Enter the name of a person who needs to be in notification sender.

6. Click **Submit** to add an Email configuration.

## Configuring vRA

## In this Section

Topic	Description
<a href="#">Importing Blueprints</a>	This section describes the details to import the XAAS blueprints.
<a href="#">Configuring Day-1 Workflows</a> (Optional)	This section describes the details to configure vRA for Day-1 workflows. If Day-1 Workflows are not required, this section can be skipped.

## Importing Blueprints

This section describes the details to import the XAAS blueprints.

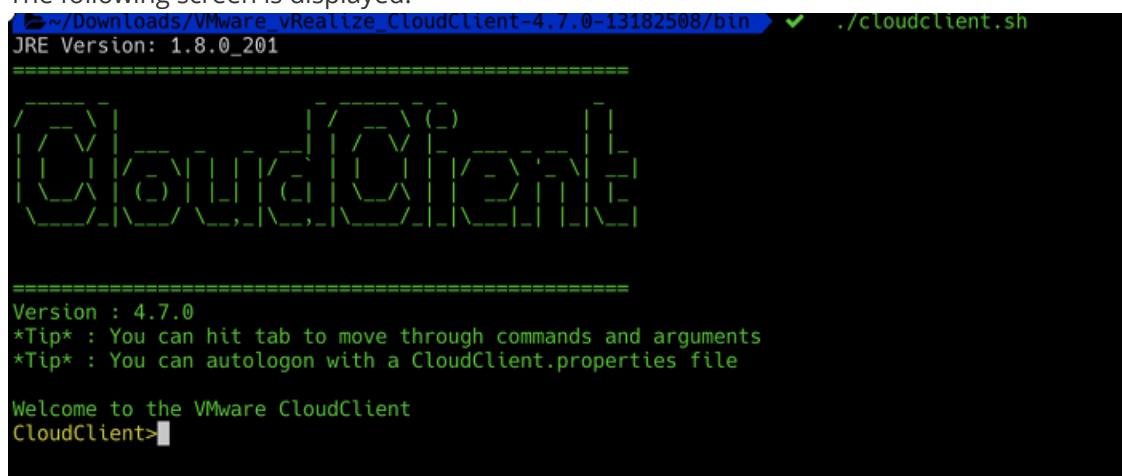
### Prerequisites

- Cohesity vRO Plugin - Ensure that the plugin is installed and configured on the vRO. Click [here](#) for the detailed procedure.
- [Cloud Client](#) - The vRealize command line utility must be available to import pre built blueprints and use cases in vRA.

### Procedure

1. Download the Cohesity vRA Blueprint file available in the [repository](#).
2. Launch Cloud Client instance on your local system by executing `bin/cloudclient.bat` (for windows) or `bin/cloudclient.sh` for OSX / Linux.

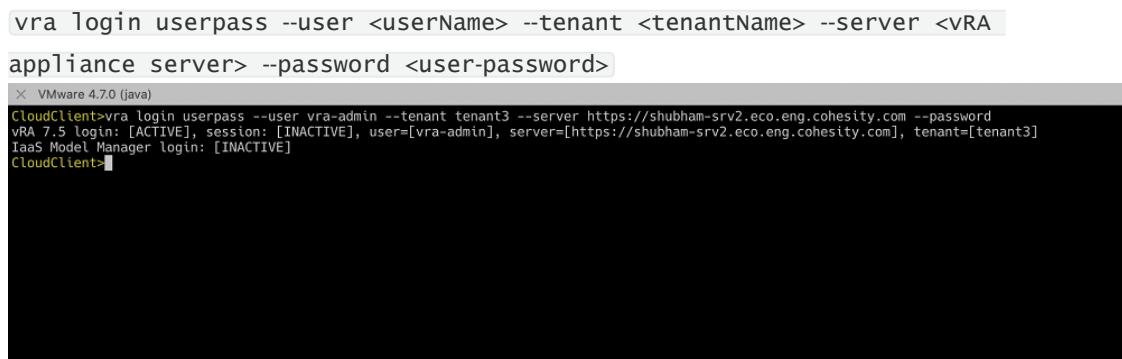
The following screen is displayed.



```
~/Downloads/VMware_vRealize_CloudClient-4.7.0-13182508/bin ./cloudclient.sh
JRE Version: 1.8.0_201
=====
[VMWARE] [VMWARE] [VMWARE]
=====
Version : 4.7.0
*Tip* : You can hit tab to move through commands and arguments
*Tip* : You can autologon with a CloudClient.properties file

Welcome to the VMware CloudClient
CloudClient>[
```

3. Login to the vRA appliance and vRA infrastructure server using the following command.



```
vra login userpass --user <userName> --tenant <tenantName> --server <vRA
appliance server> --password <user-password>
VMware 4.7.0 (java)
CloudClient>vra login userpass --user vra-admin --tenant tenant3 --server https://shubham-srv2.eco.eng.cohesity.com --password
vRA 7.5 login: [ACTIVE], session: [INACTIVE], user=[vra-admin], server=[https://shubham-srv2.eco.eng.cohesity.com], tenant=[tenant3]
IaaS Model Manager login: [INACTIVE]
CloudClient>
```

4. Import the blueprint file using the following command.

```
vra content import --path <path-to-zip-file> --resolution OVERWRITE --precheck
```

**WARN**

```

CloudClient>vra content import --path /Users/shubham.kumar/Downloads/Cohesity/39c04589-065e-4d60-bea8-49f043163c02.zip --resolution OVERWRITE --precheck WARN
+-----+
|Notification|
+-----+
* Performing import precheck for [/Users/shubham.kumar/Downloads/Cohesity/39c04589-065e-4d60-bea8-49f043163c02.zip]. Note this operation does not import any content.

+-----+
|Import Precheck Result|
+-----+
SUCCESS : Import precheck finished Success..
* 18 content(s) were validated successfully.
* Nothing was imported.

+-----+
|Notification|
+-----+
* Importing [/Users/shubham.kumar/Downloads/Cohesity/39c04589-065e-4d60-bea8-49f043163c02.zip]. Note this operation will import the given content unless it encounters failures.

+-----+
|Import Result|
+-----+
SUCCESS : Import finished Success..
* 18 content(s) were imported successfully.

```

5. To verify if the import was successful, in VRA, navigate to **Design > XaaS > XaaS Blueprints**.

Name	Description	Status
Add Unprotected VM to Protection Job	Adds an unprotected VM to given Protection Job	Published
Azure Machine	Creates new Azure virtual machine	Published
Clone Virtual Machine	This is the workflow to clone virtual machine.	Published
Move VM to New Protection Job	Move VM from one Protection Job to new Protection Job	Published
Recover Files or Folders	This is the workflow to restore selected files or folders.	Published
Remove VM from Protection Job	Removes Virtual Machine from the Protection Job	Published
Restore Virtual Machine	This is the workflow to restore virtual machine.	Published
Run Protection Job on Demand	Run Protection Job on Demand	Published

6. Navigate to **Design > XaaS > Resource Actions** to confirm successful import of Resource Actions.

Name	Description	Resource	Status
Cohesity - Add to protection job	Adds an unprotected VM to given Protection Job	IaaS VC VirtualMachine	Published
Cohesity - Change Protection Job	Moves VM from one Protection Job to new Protection Job	IaaS VC VirtualMachine	Published
Cohesity - Clone Machine	This is the workflow to clone virtual machine.	IaaS VC VirtualMachine	Published
Cohesity - Create Snapshot	Run Protection Job for the VM on Demand	IaaS VC VirtualMachine	Published
Cohesity - Recover Files/Folders	This is the workflow to restore selected files or folders.	IaaS VC VirtualMachine	Published
Cohesity - Remove From Protection Job	Removes Virtual Machine from the Protection Job	IaaS VC VirtualMachine	Published
Cohesity - Restore Virtual Machine	Restore Cohesity virtual machine.	IaaS VC VirtualMachine	Published

**Note:** Ensure that the various users are entitled to the newly imported catalog items and resource actions. Click [here](#) for more details.

## Configuring Day 1 Workflows

You need to perform the following only if you have to configure vRA for Day-1 workflows. Else, this section can be skipped.

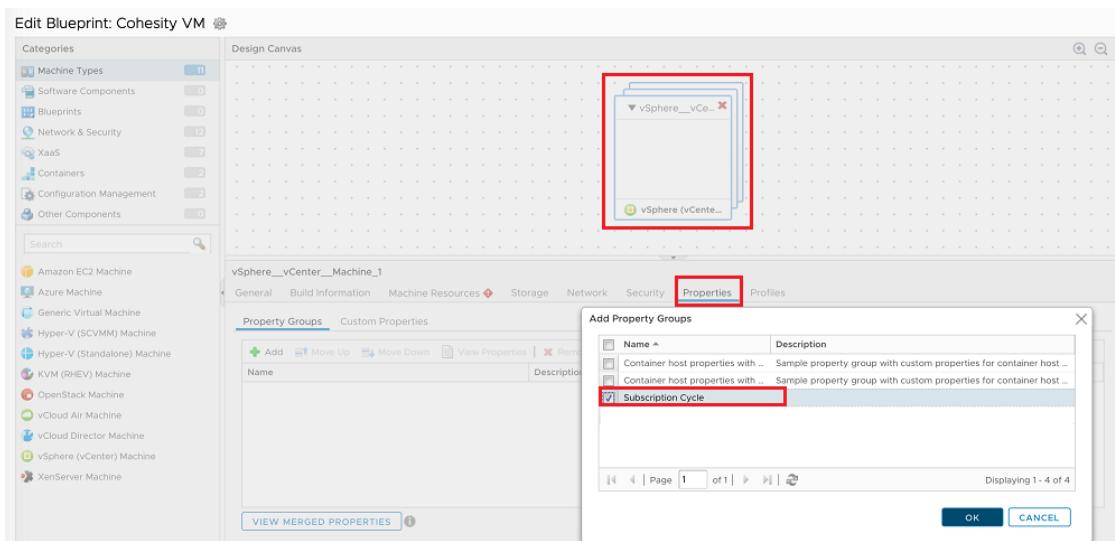
By configuring Day 1 Workflows, the VMs are added to the specified protection job when newly provisioned from VRA or removed from the protection group when the VM is destroyed.

## Assigning Properties to Blueprint

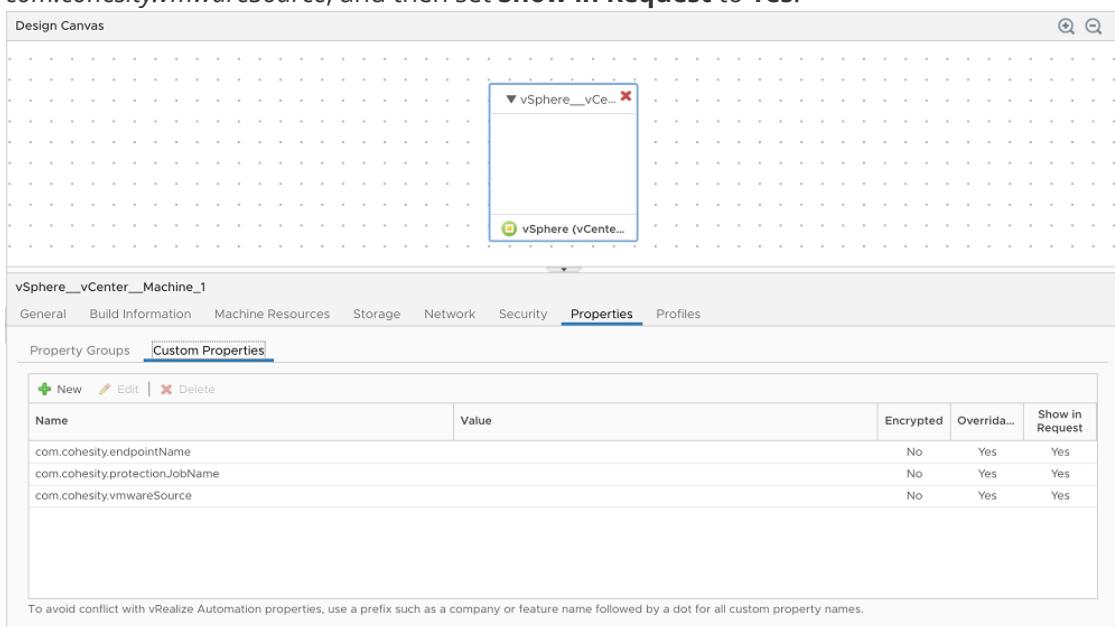
### Procedure

This section describes the steps you need to perform to configure vRA property definition and groups.

- In the **Design** tab, select **Blueprints**.
- Select an existing blueprint from the **Blueprints** pane.
- In the **Design Canvas** page, click the vSphere machine component (highlighted on the top of the page) and click the **Properties** tab. Add the property group **Subscription Cycle**.



4. Click the **Custom Properties** tab.
5. Add `com.cohesity.endpointName`, `com.cohesity.protectionJobName`, and `com.cohesity.vmwareSource`, and then set **Show in Request** to Yes.



6. Click **SAVE** to save the changes.

## Configuring Event Subscription

This section describes the steps you need to perform to create and configure event subscription.

### Procedure

1. Click **Administration > Events > Subscriptions**.

2. To create a new workflow subscription, click the **New** icon.

The screenshot shows the vRealize Automation Administration interface. The left sidebar lists various management categories like Approval Policies, Directories Management, and Catalog Management. Under the 'Subscriptions' category, a red box highlights the 'New' button in the top right corner of the main content area. The main content area displays a table for existing subscriptions, with one entry 'vRO Configuration' visible.

3. Select **Machine Provisioning** in the **Event Topic** page. Click **Next**.

The screenshot shows the 'New Workflow Subscription' page under the 'Event Topic' tab. On the left, a red box highlights the 'Machine provisioning' option in the list of event topics. The right side shows detailed information about the selected topic, including its schema and properties. At the bottom, there are 'NEXT >' and 'FINISH' buttons.

4. In the **Conditions** tab, select the following values and click **Next**.

- Run based on conditions = All of the following.
- Data > Blueprint Name = Cohesity (blueprint name to provision VM)
- Data > Lifecycle State >Lifecycle State Name = VMPSMasterWorkflow32.MachineProvisioned

- Data > Lifecycle State > State phase = POST

New Workflow Subscription

Event Topic **Conditions** Workflow Details

Specify whether the workflow should be run for all events or based on conditions.

Run for all events  
 Run based on conditions

All of the following

Data > Blueprint name Equals Cohesity  
Data > Lifecycle state ... Equals VMPSMasterWorkflow3...  
Data > Lifecycle state ... Equals POST

Add expression

< BACK NEXT > FINISH CANCEL

5. In the **Workflow** tab, select the workflow from Orchestrator and add this DAY-1 workflow of **Add Multiple VMs to Protection Job**.

New Workflow Subscription

Event Topic Conditions **Workflow** Details

Select a workflow:

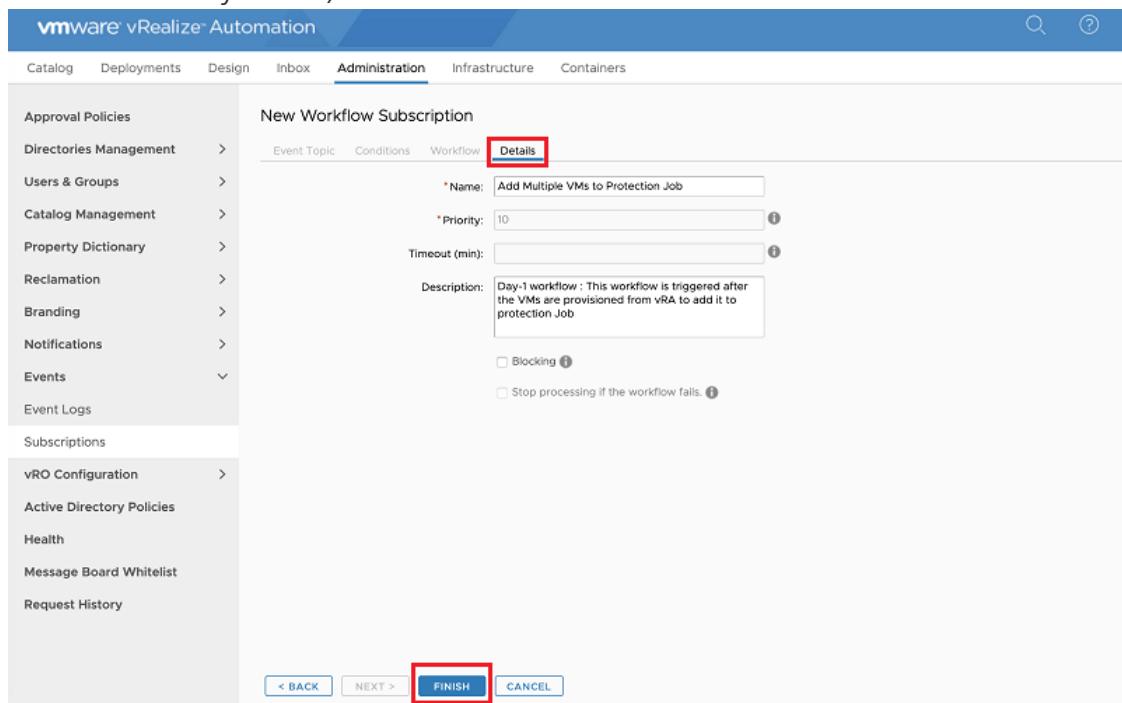
- Orchestrator
  - Library
  - AMQP
  - AMQP Samples
  - Azure
  - Cohesity
  - Configuration
  - Day-1**  Add Multiple VMs to Protection Job
  - Remove VM from All Protection Jobs
  - Protection Job
  - Utilities
- Configuration
- Data Management
- Data Management Samples
- Dynamic Types
- HTTP-REST
- HTTP-REST Samples
- JOB
- Locking
- Mail
- Microsoft
- NSX
- Orchestrator
- PowerShell

Selected workflow:

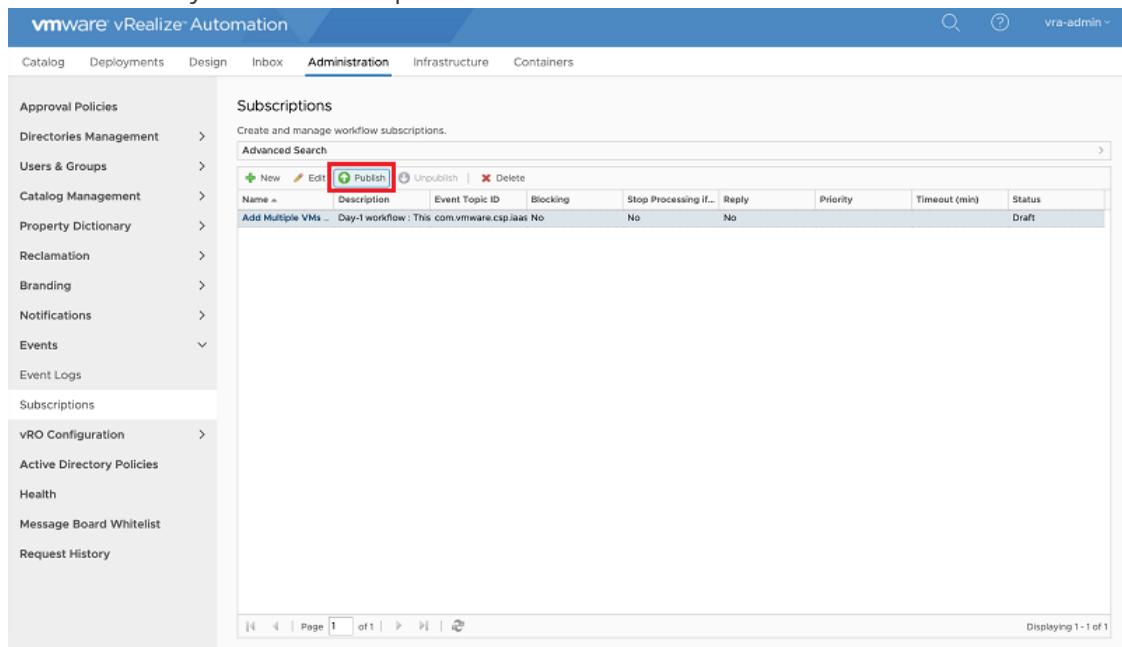
Name:	Add Multiple VMs to Protection Job
Description:	Day-1 workflow : This workflow is triggered after the VMs are provisioned from vRA to add it to protection Job
Input parameters:	
Name	Type
payload	Properties
Displaying 1-1 of 1	
Output parameters:	
Name	Type
protectionJobUpdated	CS:ProtectionJob
Displaying 1-1 of 1	

< BACK NEXT > FINISH CANCEL

6. In the **Details** tab, a new Subscription with a relevant name is displayed (It will use the Workflow name by default). Click **Finish**.



7. Select the newly created subscription and click **Publish**.



## Remove VM from Protection Job

### Procedure

To remove VM from Protection Job when VM is destroyed:

1. Click **Administration > Events > Subscriptions**.

2. Click the **New** icon and select **Machine Provisioning** in the **Event Topic** page.

3. In the **Conditions** tab, select the following and click **Next**.

- *Run based on conditions = All of the following.*
- *Data > Blueprint Name = Cohesity (Blueprint name to the provision VM)*
- *Data > Lifecycle State > Lifecycle State Name = VMPSMasterWorkflow32.UnprovisionMachine*
- *Data > Lifecycle State > State phase = PRE*

4. Select the workflow from Orchestrator and select the **DAY-1** workflow of **Remove VM from All Protection Jobs** in this page.

5. In the **Details** tab, enter the new **Subscription Name** (It will use the Workflow name by default) and then click **Finish**.

6. Select the newly created subscription and publish it.

The screenshot shows the vRealize Automation Administration interface. On the left, there's a sidebar with various management categories like Approval Policies, Directories Management, and Catalog Management. The main area is titled 'Subscriptions' with a sub-header 'Create and manage workflow subscriptions.' It includes an 'Advanced Search' section and a table with columns: Name, Description, Event Topic ID, Blocking, Stop Processing if..., Reply, Priority, Timeout (min), and Status. A row in the table is highlighted with a red box around the 'Remove VM from...' button. Buttons at the top of the table include 'New', 'Edit', 'Publish' (which is also highlighted with a green box), 'Unpublish', and 'Delete'.

After you have completed the above configurations, click the **Cohesity Provision VM**.

**Note:** Here, **Cohesity Provision VM** is given as an example. This name could differ based on the client's configuration.

The screenshot shows the vRealize Automation Catalog interface. The 'Catalog' tab is selected, showing 1 item. The search bar has 'On behalf of:' and 'Search users'. Below the search bar is a 'Search for catalog items by name or description' input field and a 'Sort: Name (ascending)' dropdown. A single item is listed: 'Cohesity Provision VM' (Linux VM, Business group: CSBusiness, Service: Ubuntu VM). At the bottom of the card, there's a blue 'REQUEST' button.

## Executing Protection Group Workflows

You can execute the following actions in the Day-2 workflows. These workflows can be executed as a XAAS or resource actions. To execute the workflow, you need certain privileges. See [Workflow Execution Privileges](#) for details.

### In This Section

Topic	Description
<a href="#">Adding a Protection Source (XAAS)</a>	This section describes the details to add a new physical or hypervisor type protection source.
<a href="#">Adding Physical Server to Protection Job (XAAS)</a>	This section describes the details to add a physical machine instance to a protection job
<a href="#">Adding an unprotected VM to protection group (XAAS)</a>	This section describes the details to add an unprotected VM to a Protection Group.
<a href="#">Cloning a VM (XAAS)</a>	This section describes the details to clone a Virtual Machine.
<a href="#">Moving a VM to a New Protection Job (XAAS)</a>	This section describes the details to move a VM to a new protection job.
<a href="#">Removing a Protection Source (XAAS)</a>	This section describes the details to remove a VMware or a physical server as a protection source.
<a href="#">Removing Physical Server from Protection Job (XAAS)</a>	This section describes the details to remove a physical server instance from its protection job.
<a href="#">Removing a VM from a Protection Job (XAAS)</a>	This section describes the details to remove a VM from a protection job.
<a href="#">Removing VM Tag from Protection Job</a>	This section describes the details to unprotect the associated VMware tags.
<a href="#">Deleting a Protection Job (XAAS)</a>	This section describes the details to delete a protection job object.
<a href="#">Restoring a Virtual Machine (XAAS)</a>	This section describes the details to restore a Virtual Machine.
<a href="#">Executing a Protection Job on Demand (XAAS)</a>	This section describes the details to run a protection job on demand.
<a href="#">Recovering Files or Folders (XAAS)</a>	This section describes the details to recover a file or a folder.
<a href="#">Upgrading Cohesity Agent (XAAS)</a>	This section describes the details to upgrade a Cohesity Agent.
<a href="#">Generating Reports (XAAS)</a>	This section describes the details to email reports.

Topic	Description
<a href="#">Executing a Protection Job on Demand</a> (Resource Action)	This section describes the details to run a protection job as a Resource Action in vRA.

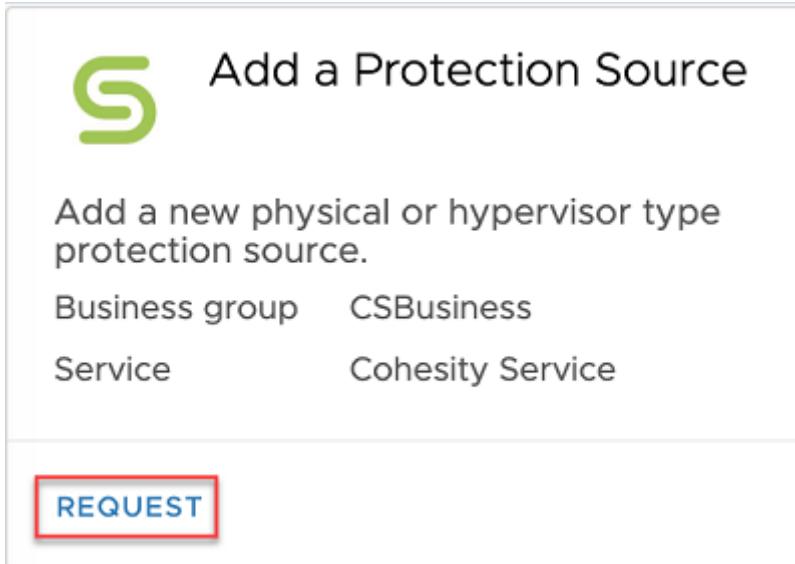
**Note:** The steps to execute a protection job on demand as a XAAS and a resource action has been captured in this section. All the other workflows can also be similarly executed either as a XAAS or a resource action.

## Adding a Protection Source

### Procedure (XAAS)

To add a new physical or hypervisor type protection source:

1. Log in to vRA using valid credentials. The list of Catalog Items are displayed in the Catalog Dashboard.  
Ensure that you have the necessary **Entitlements** to **Cohesity Catalog Items**.  
To access **Entitlements**, in vRA go to **Administration > Catalog Management > Entitlements**.
2. Click **REQUEST** on **Add a Protection Source**.



Add a Protection Source

Add a new physical or hypervisor type protection source.

Business group	CSBusiness
Service	Cohesity Service

**REQUEST**

3. Specify the initial **Cohesity Connection** along with the **Source Type**.  
The Source Type can be a **Physical Server** or **Hypervisor**.
  - o Physical Server:

1. On selecting a **Physical Server**, a new tab called **Physical Host Config** is displayed.

The screenshot shows a software interface for adding a protection source. At the top, there's a header with a 'S' icon and the text 'Add a Protection Source'. To the right of the header is a 'Business group' dropdown set to 'CSBusiness'. Below the header, there are two tabs: 'Initial Config' (which is selected) and 'Physical Host Config'. Under 'Initial Config', there are two required fields: 'Cohesity Connection' (set to 'CS Cluster [ id=CS Cluster ]') and 'Source Type' (set to 'Physical Server'). At the bottom of the screen are two buttons: 'SUBMIT' and 'CANCEL'.

2. Specify the following details:

Parameter	Description
Hostname or IP Address	Enter the hostname or the IP address of the physical machine. Note: Ensure that Cohesity agent is installed on this machine.
OS Type	Select the appropriate OS type as Host or WindowsCluster. By default, Host is selected.
Environment	Select the environment as Physical which is selected by default.
Physical Host	Select the operating system of the host machine as Linux, Windows, AIX, or Solaris.

**S Add a Protection Source** | Business group CSBusiness ▾

Initial Config **Physical Host Config**

\* Hostname or IP Address: myhost.mycompany.com

\* OS Type: Host

\* Environment: Physical

\* Physical Host: Linux

<None>

Linux

Windows

AIX

Solaris

**SUBMIT** **CANCEL**

3. Click **Submit**.

o Hypervisor:

1. On selecting **Hypervisor**, a new tab called **Hypervisor Config** is displayed.

**S Add a Protection Source** | Business group CSBusiness ▾

Initial Config **Hypervisor Config**

\* Cohesity Connection: CS Cluster [ id=CS Cluster ]

\* Source Type: Hypervisor

**SUBMIT** **CANCEL**

2. Specify the following details:

Parameter	Description
-----------	-------------

Parameter	Description
Environment	Select the environment to be a VMware or a HyperV.
Hypervisor Source Type	This option is displayed <b>only</b> if the environment is <i>VMware</i> . The hypervisor source type can be selected as VCentre or Standalone host. Standalone host indicates the standalone ESXI host entity in a VMware protection source type.
Hostname or IP Address	Specify the VCentre hostname or corresponding IP address.
Username	Enter the username of the VCentre.
Password	Enter the corresponding password of the VCentre.

Add a Protection Source | Business group CSBusiness

Initial Config Hypervisor Config

Environment: VMware

\* Hypervisor Source Type: VCenter

\* Hostname or IP Address: vcenter.host.mycompany.com

\* Username: administrator

\* Password: \*\*\*\*\*

SUBMIT CANCEL

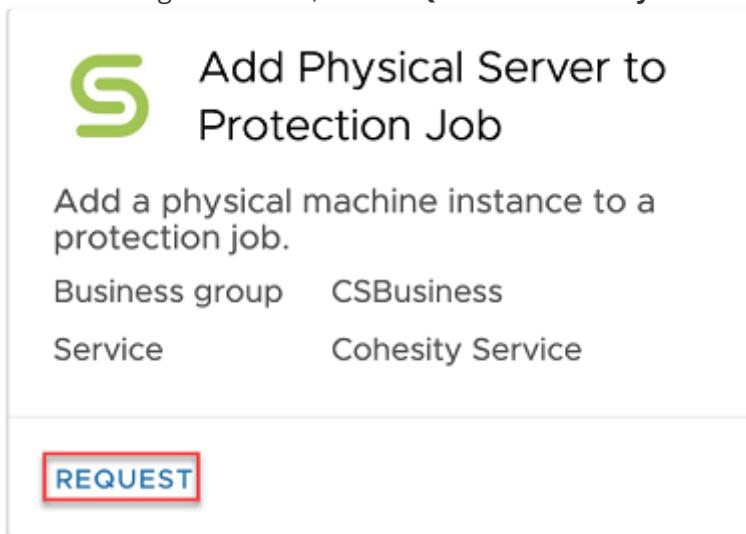
3. Click **Submit**.

## Adding Physical Server to Protection Job

### Procedure (XAAS)

To add a physical machine instance to a protection job:

1. In the Catalog Dashboard, click **REQUEST** on **Add Physical Server to Protection Job**.



2. Select the **Cohesity Endpoint** from the drop down list, and click **Submit**.

3. Under **Cohesity Parameters** tab, select **Protection Type** to be **File Based** or **Block Based**.

In case of File based, specific volumes of drives can be selected for Protection and in case of Block based, the entire physical machine is protected.

Below is the **Configuration** for **File Based** Protection Type:

Add Physical Server to Protection Job | Business group CSBusiness ▾

Endpoint Config Cohesity Parameters Protection Job Config

② \* Protection Type: File Based

③ \* Unprotected Physical Server: physicalServer.mycompany.com [ id=CS Cluster::85... ]

Volumes Mounted: C:\

Volumes Mounted: +

④ \* Protection Paths: C:\

⑤ Excluded Paths: +

C:\temp

⑥ Create New Protection Job: Yes

**SUBMIT** **CANCEL**

The screenshot shows a configuration page for adding a physical server to a protection job. The 'Cohesity Parameters' tab is active. Key settings include:

- Protection Type: File Based
- Unprotected Physical Server: physicalServer.mycompany.com
- Volumes Mounted: C:\
- Protection Paths: C:\ (with a green plus icon)
- Excluded Paths: C:\temp (with a green plus icon)
- Create New Protection Job: Yes

At the bottom, there are 'SUBMIT' and 'CANCEL' buttons.

Below is the **Configuration** for **Block Based** Protection Type:

Add Physical Server to Protection Job | Business group CSBusiness ▾

Endpoint Config Cohesity Parameters Protection Job Config

\* Protection Type: Block Based

\* Unprotected Physical Server: physicalServer.mycompany.com [ id=CS Cluster::822... ]

Volumes Mounted: C:\

Create New Protection Job: Yes

**SUBMIT** **CANCEL**

4. Select the corresponding **Physical Server Instance** from the drop down list.

**Note:** Only the physical servers that are not protected will be displayed in the drop down.

5. Only in case of **File based Protection Type**, confirm the drives to be protected in

**Protection Path.**

You can also click **Add** icon to add other drives to be protected.

**Note:** If the Protection Type is block based, then the entire physical server is protection and not specific to any drives.

6. To create a new protection job, click **Yes**. A new tab **Protection Job Config** is displayed. Provide all the configuration details and proceed.

Add Physical Server to Protection Job | Business group CSBusiness ▾

Endpoint Config Cohesity Parameters **Protection Job Config**

\* Job Name: Physical Server Job

\* Policy: Gold [ id=eyJpZCI6IjY5MTExMDI2MjE2NTg2MzI6MT... ]

\* Storage Domain: DefaultStorageDomain [ id=CS Cluster::5 ]

\* Timezone: Etc/UTC (+00:00)

\* Start Time (HH:MM format): 06:14

Advanced Configuration: No

**SUBMIT** **CANCEL**

## Add Physical Server to Protection Job

Business group CSBusiness

Endpoint Config Cohesity Parameters **Protection Job Config**

• \* Start Time (HH:MM format): 06:14

• Advanced Configuration: Yes

• \* QoS Policy: Backup HDD

• Source Side Deduplication: No

• Indexing: No

• SLA Incremental (minutes): 60

• SLA Full (minutes): 120

• Alerts:

- Success
- Failure
- Sla Violation

• \* Priority: Medium

• Email Recipients: +  
No data selected

**SUBMIT** **CANCEL**

7. To select from existing Protection jobs, choose **No** for **Create New Protection Job** and select the corresponding job from the drop down.

8. Click **Submit**.

## Adding an Unprotected VM to Protection Group

### Procedure (XAAS)

To add an unprotected VM to a protection job:

1. In the Catalog Dashboard, click **REQUEST** on **Add Unprotected VM to Protection Group**.

The screenshot shows a dialog box titled "Add Unprotected VM to Protection Job". It features a large green "S" icon on the left. The main title is "Add Unprotected VM to Protection Job". Below it is a description: "Adds an unprotected VM to given Protection Job". There are two configuration fields: "Business group" set to "CSBusiness" and "Service" set to "Cohesity Service". At the bottom is a prominent red-bordered button labeled "REQUEST".

2. From the **Endpoint Config** tab, select the **Cohesity Endpoint** from the drop down list.
3. Click **Cohesity Parameters** tab, and select the **vCenter** from the drop down and select the specific **Virtual Machines** to be protected by moving the VMs from left to right pane.  
**Note:** In the drop down list for Virtual Machines, only the unprotected VMs are displayed. However, to change this default behaviour and to allow VMs to be protected by multiple jobs, you can log in to vRealize Orchestrator, navigate to find the Cohesity library > Protection Job > Add unprotected VM to Protection Group and edit the workflow. Search for **allowDuplicates** attribute and set the field to **Yes**.
4. You can also choose to select the **Protect VMware Tags** option. On selecting this option, the VMware tags that are not used by any other protection job are displayed.  
**Note:**
  - The VMware tags are displayed only if it is assigned to at least one or more VMs. Unassigned VM tags will not be displayed.
  - You can also choose to select only the VMware tags and not select any Virtual Machines from the list.
  - If you select the Virtual Machines and not select the VMware tags, then only the selected VMs will be protected and the tags will not be protected.

5. Choose to create a **New Protection Job** by selecting **Yes/No**.

If you have selected Yes, then a new tab **Protection Job Config** is displayed.

Add Unprotected VM to Protection Job | Business group CSBusiness

Endpoint Config Cohesity Parameters

vCenter: vc-67.eco.eng.cohesity.com [ id=10.2.37.188::1 ]

VM Search (Regex supported, use '\*' for all VMs): \*

Virtual Machines:

- 1-VM2-x7Mg [ id=eyJpZCI6MjA1 ]
- 1-VM3-r91d [ id=eyJpZCI6MTY0 ]
- 2sumeet-vm-t1\_pon-fAvs [ id=eyJpZCI6Mji1 ]
- 32vm-ms-ind1 [ id=eyJpZCI6MjI ]
- aavm1bb [ id=eyJpZCI6MjE4LC ]
- aavm2bb [ id=eyJpZCI6MjA3LC ]

Protect VMware Tags:

VMware Tags:

- ECO-Datacenter [ id=eyJwcm90Z ]

New Protection Job:

Protection Job: <None>

**SUBMIT** **CANCEL**

6. Configure all the parameters to create a new job, click **Advanced Configurations** to proceed and complete all the configurations.

**Add Unprotected VM to Protection Job** | Business group CSBusiness

Endpoint Config Cohesity Parameters **Protection Job Config**

\* Job Name: VM Ware Job

\* Policy: Bronze [ id=eyJpZCI6IjY5MTExMDI2MjE2NTg2MzI6... ]

\* Storage Domain: DefaultStorageDomain [ id=CS Cluster::5 ]

\* Timezone: Etc/UTC (+00:00)

\* Start Time (HH:MM 24 hours format): 09:06

\* Advanced Configurations:

**SUBMIT** **CANCEL**

**Add Unprotected VM to Protection Job** | Business group CSBusiness

Endpoint Config Cohesity Parameters **Protection Job Config**

\* Start Time (HH:MM 24 hours format): 09:06

\* Advanced Configurations:

\* QoS Policy: Backup HDD

\* Source Side Deduplication: No

\* Indexing: No

\* SLA Full (minutes): 120

\* SLA incremental (minutes): 60

\* Priority: Medium

\* Alerts:

Success

Failure

Sla Violation

\* Recipients:

No data selected

**SUBMIT** **CANCEL**

7. To select from existing Protection jobs, choose **No** for **Create New Protection Job** and select the corresponding job from the drop down.

8. Click **Submit**.

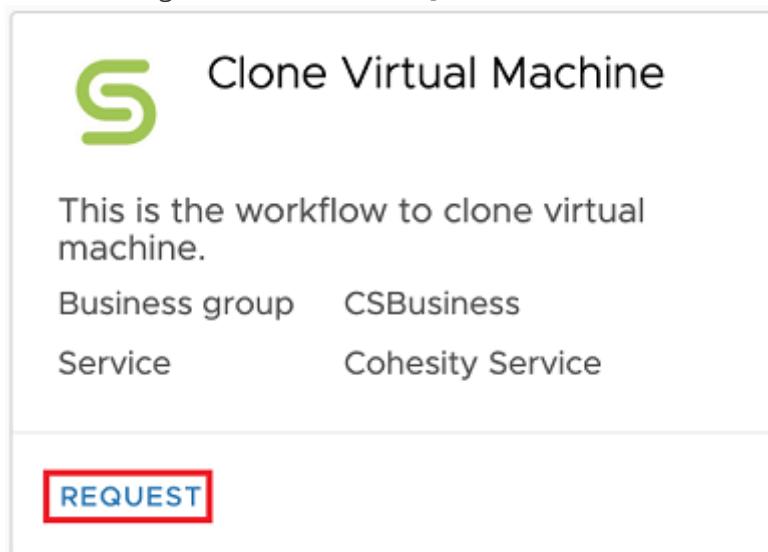
You can monitor the progress of the request in the **Deployments** tab.

## Cloning a Virtual Machine

### Procedure (XAAS)

You can clone a virtual machine as follows.

1. In the Catalog Dashboard, click **REQUEST** on **Clone Virtual Machine**.



2. Select the **Cohesity Endpoint** and the **Virtual Machine** from the drop down list.
3. Ensure that the **Machine Protected** flag in **Select Input Parameters** screen is set to **Yes**. If this is not set to **Yes**, then the machine cannot be cloned as no restore objects are

available in the cluster.

4. Select **vCenter**, **DataCenter**, **Cluster**, **Network**, **Protection Job**, **Resource Pool**, **View**, **Snapshot**, **Machine Prefix** and **Machine Suffix** from the corresponding drop down list.

 Clone Virtual Machine | Business group CSBusiness ▾

Select Input Parameters

Machine Protected: Yes

• \* vCenter: vCentre.example.com

• \* DataCenter: Datacenter [ id=CS Test 1::3 ]

• \* Cluster: ECO-cluster [ id=CS Test 1::18 ]

• Network: VLAN2144 [ id=CS Test 1::100 ]

• \* View: Demo-View

• \* Protection Job: Demo Job [ id=CS Test 1::56/41 ]

• \* Snapshot: 5/20/2019 6:37-id.57

• \* Resource Pool: testresource

• Machine Prefix.: CLONE\_

• Machine Suffix.: \_VM|

**SUBMIT** **CANCEL**

5. Click **Submit**.

## Moving a VM to a New Protection Job

### Procedure (XAAS)

You can move a VM to a new protection job as follows.

1. In the Catalog Dashboard, click **REQUEST** on **Move VM to New Protection Job**.

Move VM to New Protection Job

Move VM from one Protection Job to new Protection Job

Business group CSBusiness

Service Cohesity Service

REQUEST

2. Select the **Cohesity Endpoint** from the drop down list.
3. Under the Cohesity Parameters section, choose the **vCenter** instance, **Virtual Machine**, the **Current Protection Job**, and **New Protection Job** it must be assigned to.

**Note:** In the drop down list for Virtual Machines, only the protected VMs are displayed.

Move VM to New Protection Job | Business group CSBusiness

Select Endpoint

\* Cohesity Endpoint: Cluster [ id=Cluster ]

Select Cohesity Parameters

\* vCenter: vc-67.company.com [ id=Cluster ]

\* VM Search (Regex supported, use '\*' for all VMs): \*  
anv-centos-7.6 [ id=eyJpZCI6MTcONCwicGFyZW50SWQ  
App-tier-vms-1 [ id=eyJpZCI6MjE4MSwicGFyZW50SWQi  
App-tier-vms-2 [ id=eyJpZCI6MjE4MCwicGFyZW50SWQi  
App-tier-vms-3 [ id=eyJpZCI6MjE3OSwicGFyZW50SWQi  
Python SDK CI-CD [ id=eyJpZCI6NjE4LCJwYXJlbmRJZCI6  
vm-win16-restore-test [ id=eyJpZCI6MjYwMSwicGFyZW5  
win2k16-srv2 [ id=eyJpZCI6MTMxNCwicGFyZW50SWQiC

\* Current Protection Job:

\* New Protection Job:

SUBMIT CANCEL

4. Click **Submit**.

## Removing a Protection Source

To remove a VMware or a physical server as a protection source:

## Procedure (XAAS)

1. In the Catalog Dashboard, click **REQUEST** on Remove a Protection Source.

Remove a Protection Source

Removes a VMware/Physical env type protection source.

Business group CSBusiness

Service Cohesity Service

**REQUEST**

2. Select the **Cohesity Endpoint**, previously configured **Source Environment** (as Physical or VMware) and corresponding **Source Host/IP** from the drop down list.

S Remove a Protection Source | Business group CSBusiness

\* Cohesity Endpoint: CS Cluster [ id=CS Cluster ]

\* Source Environment: VMware

\* Source Host/IP:

<None>

vc.eng.mycompany.com [ id=CS Cluster::1 ]

vc1.eng.mycompany.com [ id=CS Cluster::950 ]

**SUBMIT** **CANCEL**

3. Click **Submit**.

**Note:** If there is already an active Protection Job that is protecting a virtual machine of vCentre, you cannot remove that virtual machine. If you wish to remove the protection source, then either the Protection job must be made inactive or the source must be removed from the Protection job.

## Removing Physical Server from Protection Job

### Procedure (XAAS)

To remove a physical server instance from its protection job:

1. In the Catalog Dashboard, click **REQUEST** on Remove Physical Server from Protection Job.

The screenshot shows a card titled "Remove Physical Server from Protection Job". Below the title is a description: "Remove a physical server instance from its protection job." Underneath, it lists "Business group" as "CSBusiness" and "Service" as "Cohesity Service". At the bottom of the card is a blue "REQUEST" button, which is highlighted with a red rectangular border.

2. Select the **Cohesity Endpoint** from the drop down list.
3. Under **Server Config** tab, select the **Physical Machine** and **Protection Job** from the drop down list.

**Note:**

- Only those physical machines that are already protected will be displayed in the drop down.
- If there is a protection job which has only 1 physical machine associated, then you cannot remove that physical machine from the job.  
A protection job will always be associated or will always protect at least one Physical machine.

The screenshot shows a configuration dialog for "Remove Physical Server from Protection Job". The "Server Config" tab is active. It displays two dropdown menus:

- \* Physical Machine: physicalServer.mycompany.com [ id=CS Cluster::85... ]
- \* Protection Job: PhyServers [ id=CS Cluster::12534 ]

At the bottom of the dialog are two buttons: "SUBMIT" and "CANCEL".

4. Click **Submit**.

## Removing a VM from a Protection Job

### Procedure (XAAS)

To remove a VM from a Protection Job:

1. In the Catalog Dashboard, click **REQUEST** on Remove VM from Protection Job.

Remove VM from Protection Job

Removes Virtual Machine from the Protecion Job

Business group CSBusiness

Service Cohesity Service

**REQUEST**

2. Select the **Cohesity Endpoint** from the drop down list.
3. Under the Cohesity Parameters section, choose an appropriate **vCenter** instance, a **Virtual Machine** and the corresponding **Protection Job**.  
**Note:** In the drop down list for Virtual Machines, only the protected VMs are displayed.
4. Select the Cohesity Parameters such as **Virtual Machine** and the corresponding **Protection Job**.

S Remove VM from Protection Job | Business group CSBusiness ▾

Select Endpoint

\* Cohesity Endpoint: Cluster 3 [ id=Cluster 3 ]

Select Cohesity Parameters

\* vCenter: vc-67.company.com [ id=Cluster 3 ]

\* VM Search (Regex supported):

\* Virtual Machine:

- <None>
- anv-centos-7.6 [ id=eyJpZCI6MTc0NCwicGFyZW50SWQ
- App-tier-vms-1 [ id=eyJpZCI6MjE4MSwicGFyZW50SWQiC
- App-tier-vms-2 [ id=eyJpZCI6MjE4MCwicGFyZW50SWQi
- App-tier-vms-3 [ id=eyJpZCI6MjE3OSwicGFyZW50SWQi
- Python SDK CI-CD [ id=eyJpZCI6NjE4LCJwYXJlbmRJZCI6
- vm-win16-restore-test [ id=eyJpZCI6MjYwMSwicGFyZW5
- win2k16-srv2 [ id=eyJpZCI6MTMxNCwicGFyZW50SWQiC

\* Protection Job:

**SUBMIT** **CANCEL**

**Note**

- In the drop down list for Virtual Machines, only the protected VMs are displayed.
  - If there is a Protection job protecting a single VM, then that VM cannot be unprotected.

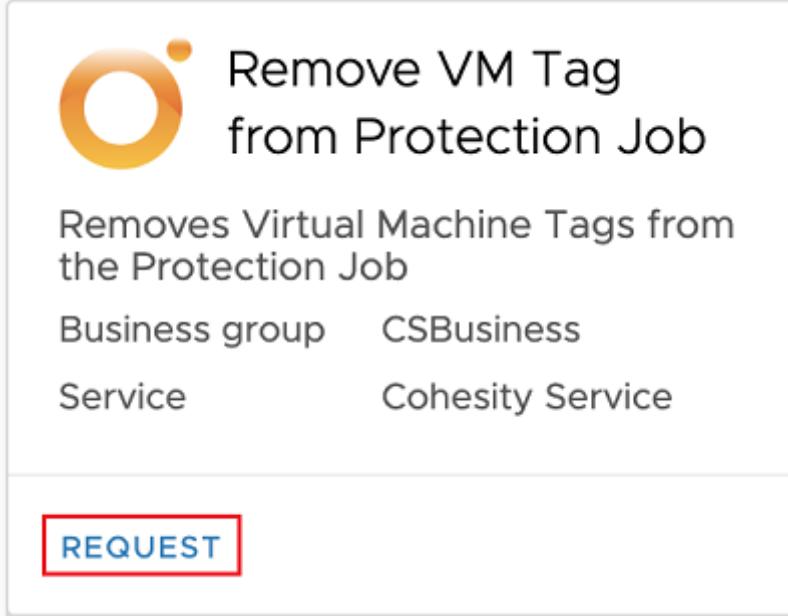
4. Click **Submit**.

## Removing VM Tag from Protection Job

### Procedure (XAAS)

To unprotect the VMware tags:

1. In the Catalog Dashboard, click **REQUEST** on **Remove VM Tag from Protection Job**.



2. Select the **Cohesity Endpoint** from the drop down list.
3. Under **Select Cohesity Parameters**, select the **vCenter** from the drop down list.
4. Choose the specific tags from the **Tag Node**. On selecting the tag, the protection job that is protecting the tags will be automatically displayed.

**Note:** Only the tags assigned to VMs will be displayed here.

 Remove VM Tag from Protection Job | Business group CSBusiness ▾

Select Endpoint

• \* Cohesity Endpoint: 10.2.37.188 [ id=10.2.37.188 ] ▾

Select Cohesity Parameters

• \* vCenter: vc-67.eco.eng.cohesity.com [ id=... ] ▾

• \* Tag Node: tag1-test [ id=eyJwcm90ZWN0aW9uU291cmNlIjp7I... ] ▾

• \* Protection Job: Tag Based Job Name [ id=10.2.37.188::1632 ] ▾

SUBMIT

CANCEL

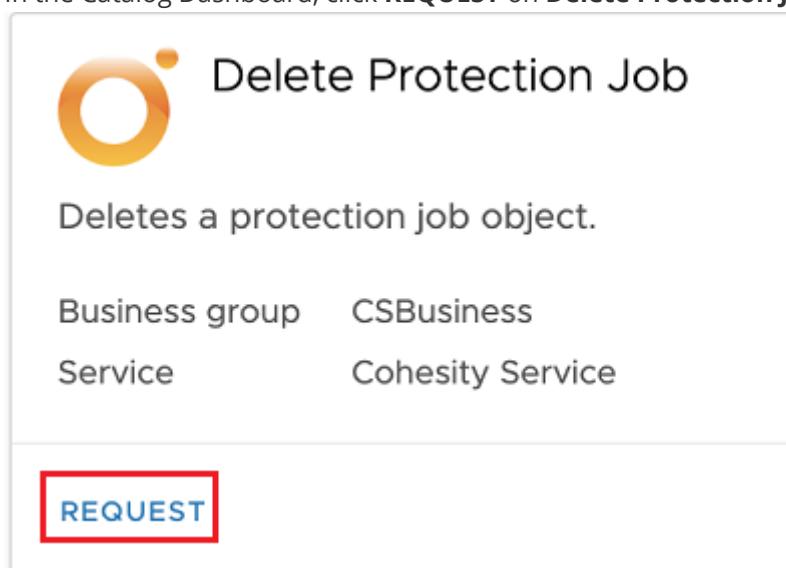
5. Click **Submit**.

## Deleting a Protection Job

### Procedure (XAAS)

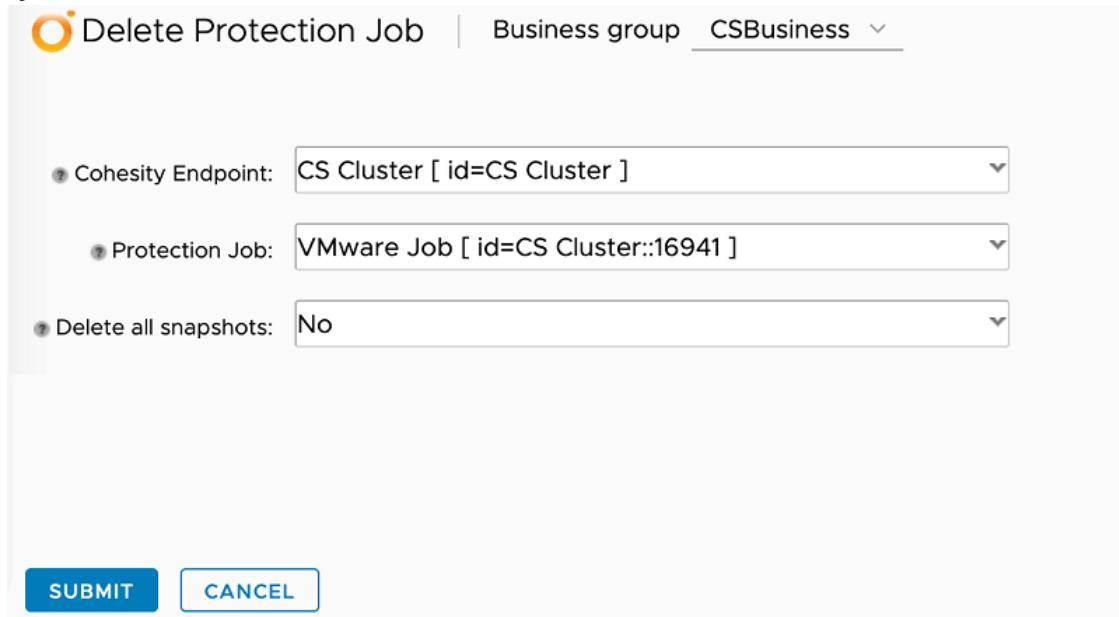
To delete a protection job object:

1. In the Catalog Dashboard, click **REQUEST** on **Delete Protection Job**.



2. Select the **Cohesity Endpoint** and the **Protection Job** that you want to delete from the drop down list.
3. Depending on the requirement, select **Yes** to **Delete All Snapshots** or **No** to retain the snapshots (selecting No will delete the protection job while the back up taken for that

system will be retained).



The dialog box shows the following fields:

- Cohesity Endpoint: CS Cluster [ id=CS Cluster ]
- Protection Job: VMware Job [ id=CS Cluster::16941 ]
- Delete all snapshots: No

At the bottom are two buttons: SUBMIT (blue) and CANCEL.

4. Click **Submit**.

## Restoring a Virtual Machine

### Procedure (XAAS)

To restore a VM:

1. In the Catalog Dashboard, click **REQUEST** on **Restore Virtual Machine**.



2. Select the **Cohesity Endpoint** and the **Backup Candidates** from the drop down list.  
**Note:** The Backup Candidates are the VMs that are already protected in the Cohesity Data

Protection.

S Restore Virtual Machine | Business group CSBusiness

Select Cohesity Endpoint and Backup Candidate Selection Restore Properties

\* Cohesity Endpoint: CS Test 1 [ id=CS Test 1 ]

Search Virtual Machine Name:

\* Backup Candidates: photon-linux [ id=CS Test 1::113 ]

- Click **Selection Restore Properties** tab and enter the protection job you want to perform the restore from in the **Protection Job** field.

Note: The list populated in the drop down of **Protection Job** may contain multiple values if the backup candidate is protected by multiple jobs.

- Select the **Snapshot** from which you want to execute the restore.
- Optionally, you can provide the **Machine Prefix** and **Machine Suffix**.
- By default, the VM is powered OFF after restore. Select as required and click **Submit**.

S Restore Virtual Machine | Business group CSBusiness

Select Cohesity Endpoint and Backup Candidate Selection Restore Properties

\* Protection Job: Demo Job [ id=CS Test 1::56/113 ]

\* Snapshots: 5/20/2019 20:30~id.142

Machine Prefix: RS\_

Machine Suffix: \_VM

Power On Machine: No

SUBMIT CANCEL

## Executing a Protection Job on Demand

### Procedure (XAAS)

To execute a Protection Job:

1. In the Catalog Dashboard, click **REQUEST** on **Run Protection Job on Demand**.

Run ProtectionJob on Demand

Business group CSBusiness

Service Cohesity Service

**REQUEST**

2. Select the **Cohesity Endpoint** from the drop down list.
3. In the **Protection Job** field, enter the protection job you want to execute.
4. In the **Run Type** field, you can select either **Regular (Incremental CBT)** or **Full (No CBT)**.

Run ProtectionJob on Demand | Business group CSBusiness

Select Endpoint

\* Cohesity Endpoint: CS Test 1 [ id=CS Test 1 ]

Select Cohesity Parameters

\* Protection Job: Demo - 2 Job [ id=CS Test 1::200 ]

\* Run Type (Specify the type of backup.): Regular (Incremental (CBT))

SUBMIT CANCEL

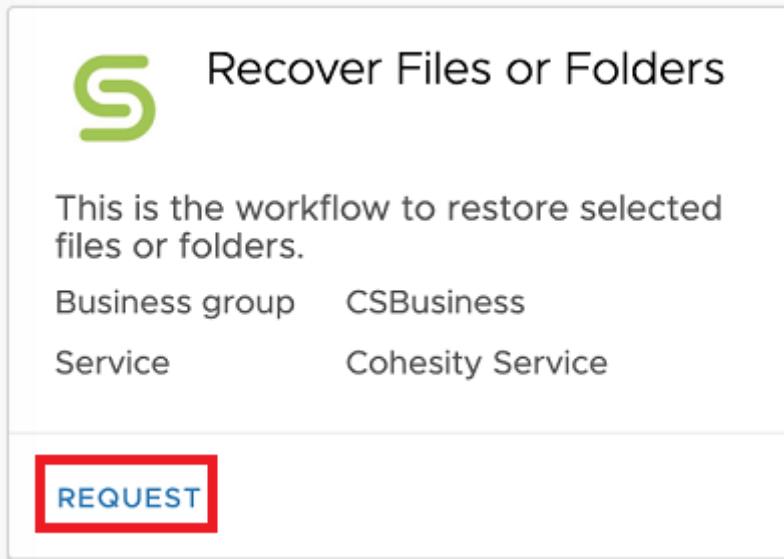
5. Click **Submit**.

## Recovering Files or Folders

### Procedure (XAAS)

To recover a file or folder:

1. In the Catalog Dashboard, click **REQUEST** on **Recover Files or Folders**.



2. Select the **Cohesity Endpoint** from the drop down list.
3. Click **Backup Candidate Config** tab, select the **Environment** from the drop down list.
4. In the **Search Virtual Machine Name** field, enter the virtual machine from which you want to recover a file or folder. A list of backup candidates is populated based on the selection.
5. Select the VM name as **Backup Candidates** and the **Protection Group** from the dropdown list.
6. Select the **OS Type** from the drop down list.
7. In the **User Name** field, provide user name for the selected VM.
8. In the **Password** field, provide password for the selected VM.
9. Select the **Recovery Method** as Agent Based or VMware Tools. The VMware Tools option is supported and effective only from Cohesity cluster version 6.5 or higher.

**Note:** The OS type and recovery method fields are related. If the OS type is Windows, then the recovery method is populated as Agent Based which is also the recommended recovery method for Windows. For other OS types, the recommended recovery method is VMware

Tools.

Catalog Deployments Design Inbox Administration Infrastructure Containers

S Recover Files or Folders | Business group BG-Group2

Cluster Config Backup Candidate Config Recover File Config

\* Environment: VMware

\* Search Virtual/Physical Machine Name: photon

\* Backup Candidate: photon-linux-demo [ id=eyJuYW1lljoiGhvdG9uLWx... ]

\* Protection Group: Important Machines [ id=eyJuYW1lljoiSW1wb3JOYW... ]

\* OS Type: Windows

\* User Name(Virtual Machine Credentials): Administrator

\* Password(Virtual Machine Credentials): .....

\* Recovery Method: Agent Based

**SUBMIT** **CANCEL**

10. In **Recovery File Config** tab:

1. In **Files or Folders** field, select option to search for files, folders or both.
2. In the **Search Files or Folders Name** field, you can provide the search text to fetch the appropriate file or folder or both from the selected protection job. The search text can be a prefix or suffix or mid name of the file or folder name.
3. Search responses such as file or folder path or both is listed in the **Files Backup Candidates** field.
4. In the **File Snapshots** field, recovery points for the selected file or folder path is listed.
5. Select **Yes** or **No** for **Recover to Original Location** parameter. If **Yes** is selected, file or folder is recovered to the original location from where it is backed up. If **No** is selected, **Recover To** field appears where you can specify the new path to recover the file or folder.
6. Select **Yes** or **No** for **Overwrite Existing File/Folder** parameter. If **Yes** is selected, file or folder is overwritten, else a new folder is created to recover the file or folder.
7. Select **Yes** or **No** for **Continue on Error** parameter. If **Yes** is selected, recovery is continued even when there is any error, else recovery stops when there is an error.
8. Select **Yes** or **No** for **Preserve Attributes** parameter.
9. Select **Yes** or **No** for **Send Email Notification**. If **Yes** is selected, the **Mail Configuration to Send Notification** tab is enabled to choose Email connection and other related parameters.
  1. In the **Email connection** field, select the Email connection which is already configured.
  2. In the **Recipients** field, add one or more Email recipients.
  3. In the **Email Subject** field, subject is auto populated. However, it can be edited.

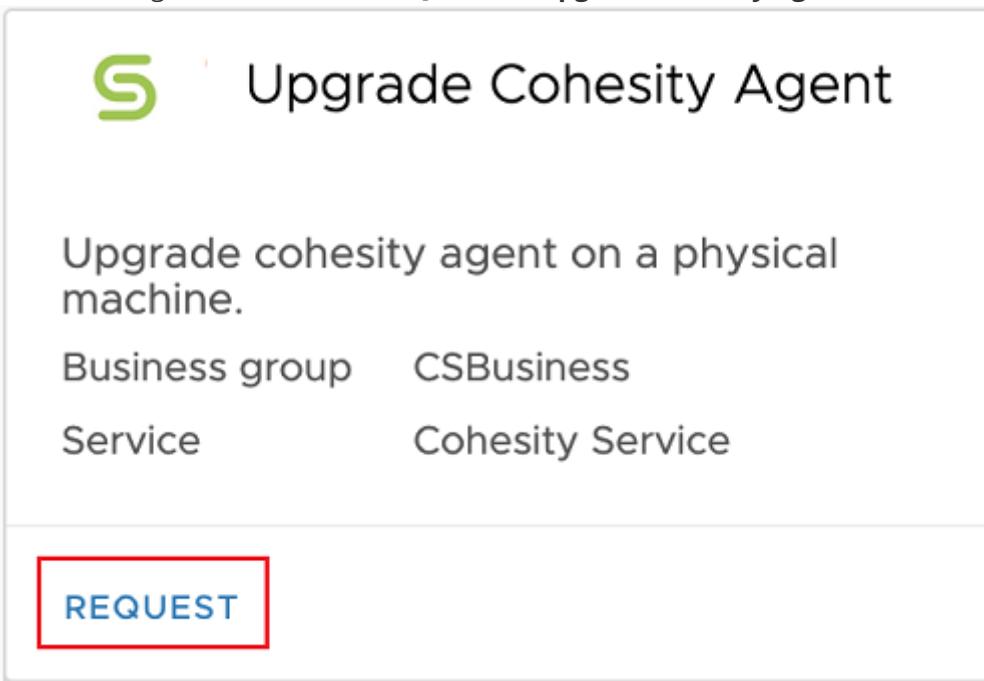
4. In the **Email Content** field, model text is auto populated in HTML format and you can edit it as per the need.
11. Click **Submit** to start the workflow execution.  
**Note:** The VM must be powered on for the workflow execution to be successful.

## Upgrading Cohesity Agent

### Procedure (XAAS)

To upgrade a Cohesity Agent:

1. In the Catalog Dashboard, click **REQUEST** on **Upgrade Cohesity Agent**.



2. Select the **Cohesity Endpoint** from the drop down list.

3. Select the **Physical Machine**.

The physical machines already registered will be displayed in the list. The **Status** and the **Upgradability** of the agent are updated accordingly. The Status reflects the current status of the agent and the upgradability indicates if the agent can be upgraded to any newer version available.

**S** Upgrade Cohesity Agent | Business group CSBusiness ▾

\* Cohesity Endpoint: Cluster 1 [ id=Cluster 1 ]

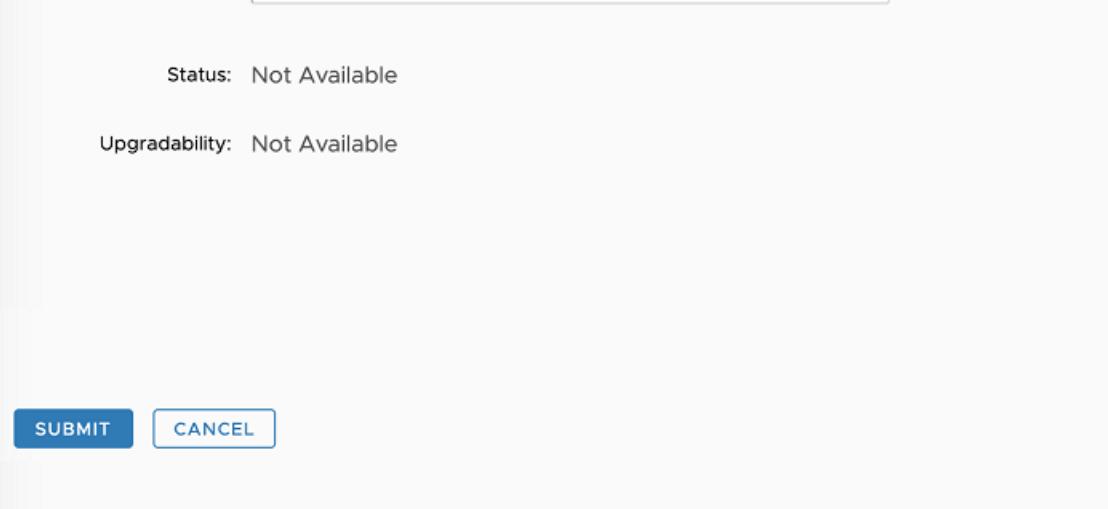
Multiple:

\* Physical Machine: Physical Machine 1 [ id=eyJpZCI6MTY1NCwibmFtZSI... ]

Status: Not Available

Upgradability: Not Available

**SUBMIT** **CANCEL**



4. If multiple option is selected, then multiple physical machines can be added.

**Note:** The **Status** and the **Upgradability** fields will not be available when multiple option is selected.

**S** Upgrade Cohesity Agent | Business group CSBusiness ▾

\* Cohesity Endpoint: Cluster 1 [ id=Cluster 1 ]

\* Multiple:

\* Physical Machines:



Physical Machine 1 [ id=eyJpZCI6I ]

**SUBMIT** **CANCEL**



5. Click **Submit**.

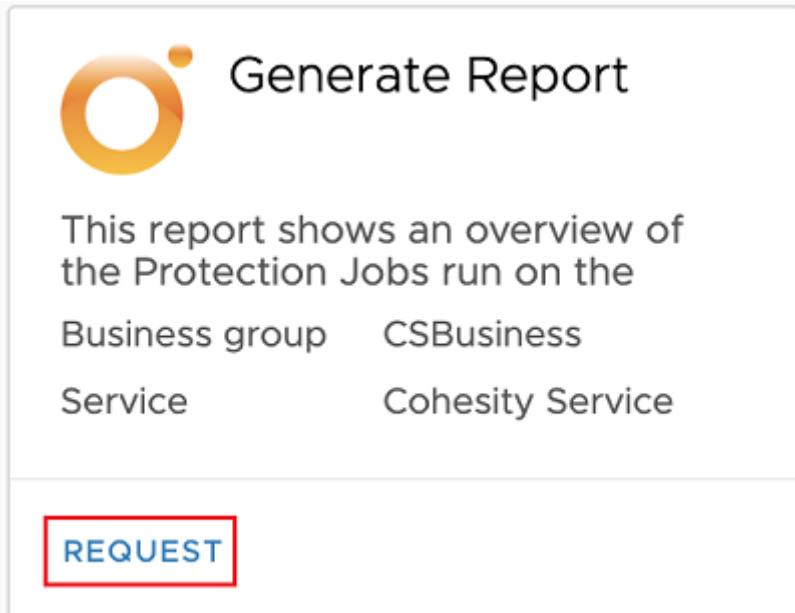
**Note:** Status of the agent upgrade request cannot be monitored through the workflow if multiple physical sources are selected.

## Generating Reports

### Procedure (XAAS)

To generate a report that provides an overview of the protection jobs:

1. In the Catalog Dashboard, click **REQUEST** on **Generate Report**.



2. Select the **Cohesity Connection** which is the cluster from where the report must be generated.
3. Under **Report Filters**, configure the **Email Recipients** IDs to which the generated report will be emailed.
4. Specify the format of the generated report (html, csv).  
**Note:** If CSV is specified, then the generated report will be sent as an attachment in the email.
5. Choose the specific **Registered Source**.  
Note: If left blank, all the registered sources in that cluster will be considered.
6. Choose any specific Protection Job or if left blank, all the protection jobs will be considered.
7. Specify the Report Time Span.  
**Note:** If you configure a value of 7, then starting from the current day, the report will be

generated for the time span of the last seven days.

Generate Report | Business group CSBusiness ▾

**Endpoint Config**

• \* Cohesity Connection: 10.2.37.188 [ id=10.2.37.188 ]

**Report Filters**

• \* Email Recipients: testmail@cohesity.com 

No data selected

• \* Format: html

• Registered Source (Leave blank for all sources):

vc-67.eco.eng.cohesity.com [ id=10.2.37.188::1 ]  
 shubham-srv5.eco.eng.cohesity.com [ id=10.2.37.188::5 ]  
 Physical Servers [ id=10.2.37.188::1135 ]

• Protection Job (Leave blank for all jobs): Important Setup Machines [ id=10.2.37.188::838 ]

• Report Time Span: 7

**SUBMIT** **CANCEL**

8. Click **Submit**.

On success, the report will be emailed to the specified Email ID.

## Executing a Protection Job on Demand as Resource Action

### Procedure (Resource Action)

To execute a Protection Job as a Resource Action in VRA:

1. In the **Deployments** tab , click on the required provisioned VM.
2. In the **Components** pane in the bottom left of the screen, click on **Actions** icon (as highlighted in the figure).

### 3. Select Cohesity-Create Snapshot.

No description

Owner	Admin User	Lease duration	1 day
Provisioned on	May 21, 2019 1:44 PM	Expires	in 23 hours
Business group	CSBusiness	Destroy date	May 24, 2019 1:44 PM
Catalog item	Cohesity		

HIDE DETAILS ▾

**Components** History

General Storage Network Security Properties Snapshots

Name: PS15  
Component: vSphere\_\_vCenter\_\_Machine\_1  
Status: On  
CPUs: 4  
Memory (MB): 4096  
Storage (GB): 16  
Description:  
Owner: vra-admin@vsphere.local  
Blueprint: Cohesity  
Compute resource: ECO-cluster

Change Lease  
Cohesity - Add to protection j...  
Cohesity - Change Protection ...  
Cohesity - Clone Machine  
**Cohesity - Create Snapshot**  
Cohesity - Recover Files/Folder...  
Cohesity - Remove From Protec...  
Cohesity - Restore Virtual Mac...  
Connect to Remote Console

4. Select the **Cohesity Endpoint** from the drop down list.

5. Ensure that the **VM Protected** flag is set to **Yes**.

If this is not set to Yes, assign the VM to a protection job first.

6. In the **Protection Job** field, enter the protection job you want to execute.

7. In the **Run Type** field, you can select either **Regular (Incremental CBT)** or **Full (No CBT)**.

#### Cohesity - Create Snapshot - PS15

Run Protection Job for the VM on Demand

##### Select Endpoint

\* Cohesity Endpoint: CS Test 1 [ id=CS Test 1 ]

##### Select Cohesity Parameters

VM Protected: Yes

\* Protection Job: Demo - 2 Job [ id=CS Test 1::200 ]

\* Run Type (Specify the type of backup.): Regular (Incremental (CBT))

SUBMIT

CANCEL

8. Click **Submit**.

To monitor the progress, log in to the Cohesity Dashboard and click **Protection** tab to view the progress.

## Multi-Tenancy Workflows

## In This Section

Topic	Description
<a href="#">Cohesity- Enable/Disable Multi Tenancy</a>	This section describes the details to enable or disable multi tenancy feature.
<a href="#">Map vRA Tenant to a new Cohesity Org</a>	This section describes the details to map a vRA tenant to a new Cohesity org.
<a href="#">Map vRA Tenant to existing Cohesity Org</a>	This section describes the details to map a vRA tenant to an existing Cohesity org.
<a href="#">Delete vRA Tenant Mapping</a>	This section describes the details to delete tenant mapping.

## Cohesity Enable Disable Multi Tenancy

Make sure to enable Multi Tenancy/Organizations on your Cohesity cluster.

### Procedure

To enable Multi-Tenancy:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > MT -Configuration > Cohesity- Enable/Disable Multi Tenancy**.
4. To start the workflow, click .
5. Select **Yes** to enable the Multi-Tenancy and click **Submit**.

On success, Multi-Tenancy will be enabled on the Cohesity cluster.

## Map vRA Tenant to a new Cohesity Org

### Procedure

To map a vRA tenant to a new Cohesity Organization:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > MT -Configuration > Map vRA Tenant to a new Cohesity Org**.
4. To start the workflow, click .
5. In the **Tenant Details** window, configure the details and select the vRA tenant. Click **Next**.  
**Note:** Only the unmapped vRA tenants are listed in the dropdown.
6. In the **Storage Domain** window, enter a domain name which is unique across Cohesity tenants. Configure other details and click **Submit**.  
**Note:** vRA Tenant users cannot access Cohesity workflows.

## Map vRA Tenant to existing Cohesity Org

### Procedure

To map a vRA tenant to a new Cohesity Organization:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
  2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
  3. Select **Library > Cohesity > MT -Configuration > Map vRA Tenant to existing Cohesity Org**.
  4. To start the workflow, click .
  5. Configure the details, select **vRA Tenant** and **Cohesity Tenant** and click **Submit**.
- Note:** Only unmapped vRA Tenants and Cohesity Tenants are listed in the dropdown. vRA Tenant users cannot access Cohesity workflows.

## Delete vRA Tenant Mapping

### Procedure

To delete all tenant mapping in vRO configuration:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
  2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
  3. Select **Library > Cohesity > MT -Configuration > Delete vRA Tenant Mapping**.
  4. To start the workflow, click .
  5. Select the Cohesity cluster, vRA Host, and vRA tenant from the dropdown list.
- Note:** Only the mapped vRA tenants are listed in the dropdown. Once a mapping is deleted, tenant users will not be able to execute CS workflows.

## Other Workflows

### In This Section

Topic	Description
<a href="#">Removing a Cohesity Endpoint</a>	This section describes the details to remove an existing Endpoint.
<a href="#">Updating a Cohesity Endpoint</a>	This section describes the details to update a Cohesity Endpoint.
<a href="#">Removing Email Configuration</a>	This section describes the details to remove the Email configuration.
<a href="#">Updating Cohesity Email Configuration</a>	This section describes the details to update an Email configuration.

## Removing a Cohesity Endpoint

### Procedure

To remove an endpoint:

1. Log in to **VMware vRealize Orchestrator**. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > Configuration > Remove a Cohesity Endpoint**.

4. To start the workflow, click . The **Remove a Cohesity Endpoint** screen is displayed.

Start Workflow : Remove a Cohesity Endpoint

Remove Cohesity Endpoint

\* Cohesity Endpoint  
 Not set

Cancel Submit

5. In the **Cohesity Endpoint** field, click the **Not set** link to select the endpoint you want to remove. The following screen is displayed.

Start Workflow : Remove a Cohesity Endpoint

Remove Cohesity Endpoint

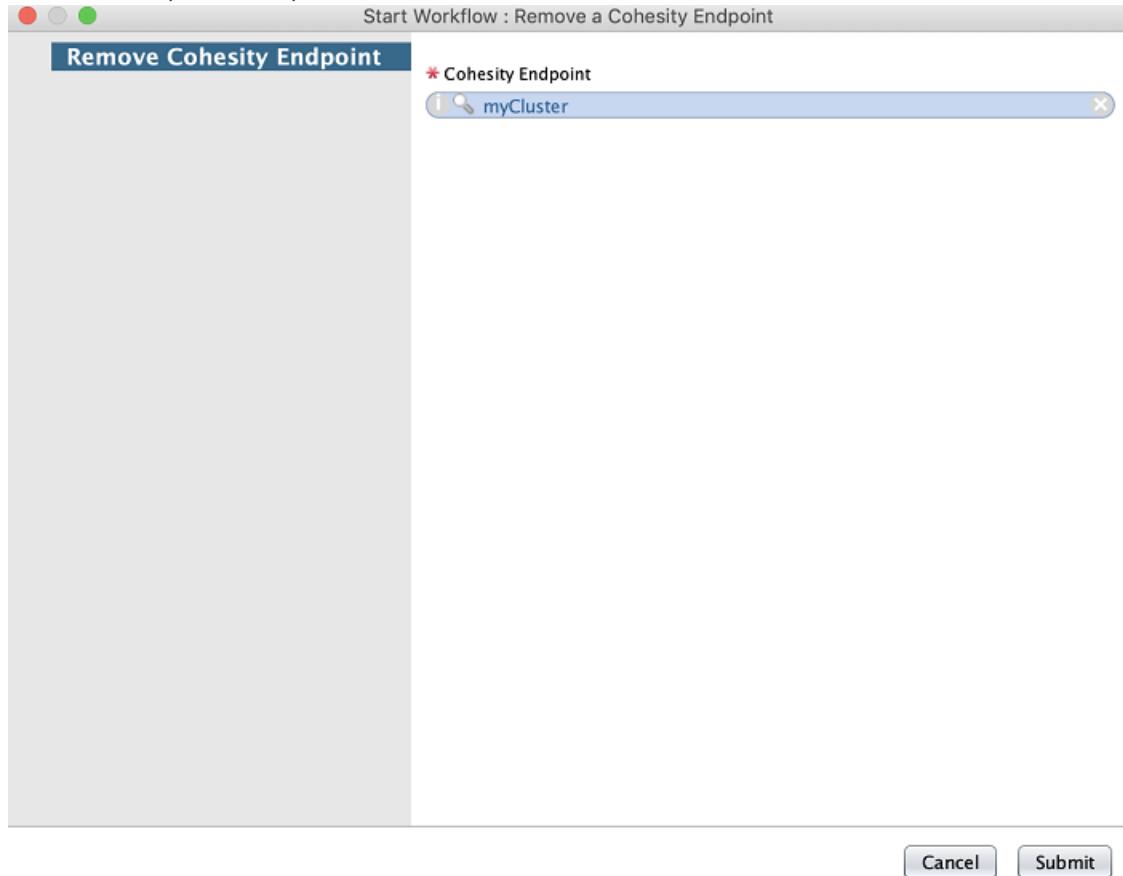
\* Cohesity Endpoint

Filter

CS:CohesityConnection	myCluster
-----------------------	-----------

Cancel Submit

6. Select the required endpoint and click **Select**.



7. Click **Submit** to remove the selected endpoint.

## Updating a Cohesity Endpoint

### Procedure

To update an endpoint:

1. Log in to VMware vRealize Orchestrator. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > Configuration > Update a Cohesity Endpoint**.

4. To start the workflow, click . The **Update a Cohesity Endpoint** screen is displayed.

The screenshot shows a software interface titled "Start Workflow : Update a Cohesity Endpoint". On the left, a vertical sidebar displays the steps: "1 Update a Cohesity Endpoint" and "1a Cohesity Endpoint". The main panel has a header "1 Update a Cohesity Endpoint" and a sub-header "1a Cohesity Endpoint". A required field "Cohesity Endpoint" is present, with a red asterisk (\*) and the status "Not set". Below the field is a search icon and a "Not set" link. At the bottom right are "Cancel" and "Submit" buttons.

5. In the **Cohesity Endpoint** field, click the **Not set** link to select the endpoint you want to update. The following screen is displayed.

The screenshot shows the same software interface as the previous step, but the "Cohesity Endpoint" field is now expanded. It contains a "Filter" input field and a list of available endpoints. One endpoint, "myCluster", is selected and highlighted. At the bottom right are "Cancel", "Back", "Next", and "Submit" buttons.

6. Select the endpoint you want to update, click **Select** and then click **Next**.

7. Enter the details you want to update and click **Submit**.

The screenshot shows a software interface for updating a Cohesity endpoint. At the top, it says "Start Workflow : Update a Cohesity Endpoint". Below that, a title bar says "1 Update a Cohesity Endpoint" with two tabs: "1a Cohesity Endpoint" (marked with a checkmark) and "1b New Settings" (marked with a red X).  
The main area contains several input fields:

- "Endpoint Name": myCluster
- "Hostname or IP address of Cohesity Cluster": cluster.cohesity.com
- "Domain Name": LOCAL
- "User Name": admin
- "Password": (empty field with a red X icon)

A yellow banner at the top right indicates "1 error - [Password], Mandatory field not set". At the bottom, there are four buttons: "Cancel", "Back", "Next", and "Submit".

## Removing Email Configuration

### Procedure

To remove Email configuration:

1. Log in to VMware vRealize Orchestrator. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > Configuration > Remove Email Configuration**.

4. To start the workflow, click . The **Remove Email Configuration** screen is displayed.

Start Workflow : Remove Email Configuration

**Remove Email Connection**

\* Email Connection Name

[Not set](#)

[Cancel](#) [Submit](#)

5. In the **Email Connection Name** field, click the **Not set** link to select the **Email configuration** you want to remove. The following screen is displayed with the available Email Configurations listed.

Start Workflow : Remove Email Configuration

**Remove Email Connection**

\* Email Connection Name

Filter |

CS:CohesityConnection	<a href="#">email config</a>
	<a href="#">myCluster</a>

[Cancel](#) [Submit](#)

6. Select the required **Email Configuration** and click **Select**.  
7. Click **Submit** to remove the selected Email configuration.

# Updating Cohesity Email Configuration

## Procedure

To update an Email configuration:

1. Log in to VMware vRealize Orchestrator. You must know the credentials to log in.
2. Select **Run** mode from the drop-down list located at the top left of the page and then click the Workflows tab.
3. Select **Library > Cohesity > Configuration > Update Email Configuration**.
4. To start the workflow, click . The **Update Email Configuration** screen is displayed.

The screenshot shows a workflow interface for 'Update Email Configuration'. The main title is '1 Update a Cohesity Email ...'. Below it, the specific step is '1a Email Configuration'. A required field, 'Email Configuration', is shown with a red asterisk and the value 'Not set'. There is a search icon next to the field. At the bottom right, there are 'Cancel' and 'Submit' buttons.

5. In the **Email Configuration** field, click the **Not set** link to select the Email configuration you want to update. The following screen is displayed with the available Email configurations

listed.

Start Workflow : Update Email Configuration

### 1 Update a Cohesity Email ...

1a Email Configuration

\* Email Configuration

Filter	
CS:CohesityConnection	email config
	myCluster

Cancel    Submit

6. Select the Email configuration you want to update, click **Select** and then click **Next**.
7. Enter the details you want to update and click **Submit**.

Start Workflow : Update Email Configuration

### 1 Update a Cohesity Email ...

✓ 1a Email Configuration  
✗ 1b New Settings

1 error - [Email Server Password], Mandatory field not set

\* Email Configuration Name

\* Email Server SMTP Host)

\* Email Server SMTP Port)

\* Email Server User Name

\* Email Server Password  
 ✗

\* From Email Id

\* From Name

Cancel    Back    Next    Submit