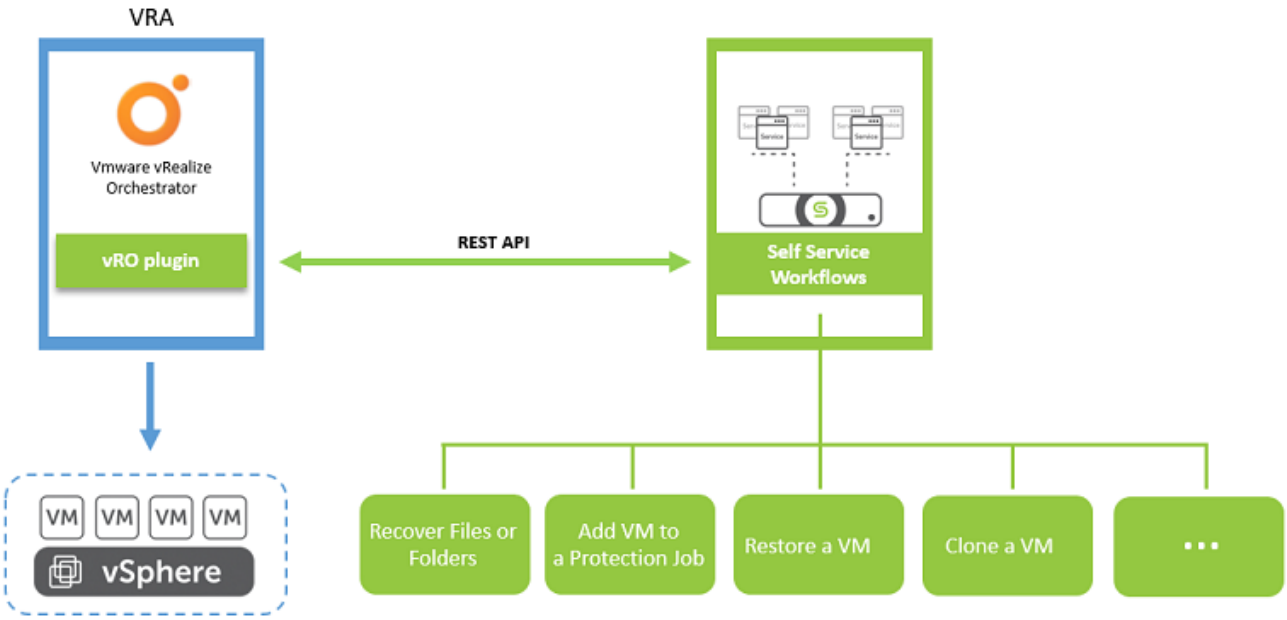
Cohesity vRO Plugin Deployment Guide

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 Group, 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. Make sure the configured user has required privileges before executing any workflows.

Custom Objects	Workflows	Privileges
Initial Configuration	Add a Cohesity Endpoint	
Day-1 Workflows	Add multiple VMs to Protection Groups	
	Remove VM from all Protection Groups	
Protection Group Workflows	Add Unprotected VM/Physical server to Protection Group	Read Cohesity Storage Domains
		View Protection Groups
		View Protection Policies

Custom Objects	Workflows	Privileges
		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
	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 Group	Manage Protection Groups
		View Protection Policies
	Delete Protection Group	Delete Protection Group
	Restore Virtual Machine	View Protection Groups
		Manage Recover Tasks
		View Recover Tasks
	Restore Virtual Disk	View Protection Groups
		Manage Recover Tasks
		View Recover Tasks
	Run Protection Group on Demand	View Protection Groups
		Protection Group Operator
	Generate Backup Summary Report	View Protection Groups
		Reporting
	Recover Files or Folders	View Protection Groups
		Manage Recover Tasks
		View Recover Tasks
	Remove Protection Source	Manage Sources

vRA supported workflows

XAAS Workflows	Resource Actions
1. Add a Protection Source	1. CS - Add VM to protection group
2. Add Physical Source to Protection Group	2. CS - Change protection group
3. Add Unprotected VM to Protection Group	3. CS - Create Snapshot
4. Clone Virtual Machine	4. CS - Recover Files or Folders
5. Delete Protection Group	5. CS - Remove VM from Protection Group
6. Generate Report	6. CS - Restore Virtual Disk
7. Move VM to new Protection Group	7. CS - Restore Virtual Machine
8. Recover Files or Folders	
9. Remove a Protection Source	
10. Remove Physical Server from Protection Group	
11. Remove VM from Protection Group	
12. Restore Virtual Machine	
13. Restore Protection on Demand	
14. Upgrade Cohesity Agent	

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	7.5 or higher	6.3 or higher
v2.1.1*, v2.2.0*	7.5 or higher	6.5, 6.4.1c

> *Multi tenancy workflows are only supported with Cohesity cluster v6.4.1c, v6.5.1 and above.

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
5. Execute Multi-Tenancy Workflows

What's New

Version	What's New	Revision Date
v2.2.0	Isolation of vRA business group backup resources through restricted users. (MT Related)	July 2020
v2.1.1	Support for multi-tenancy workflows. See Multi-Tenancy Workflows	June 2020
	This release introduces the Recovery method in Recover Files or Folders workflow.	May 2020
	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
v1.0.2	Second Draft of vRO plugin documentation. The document has been updated with the current procedures to execute workflows.	May 2019

Version	What's New	Revision Date
v1.0.1	First draft released.	Nov 2018

Installing the Cohesity vRO Plugin

In This Section

Topic	Description
Installing the Plugin	This section describes the detailed steps to install the Cohesity vRO plugin.
Removing the Plugin	This section provides information on disabling and removing the Cohesity vRO plugin.

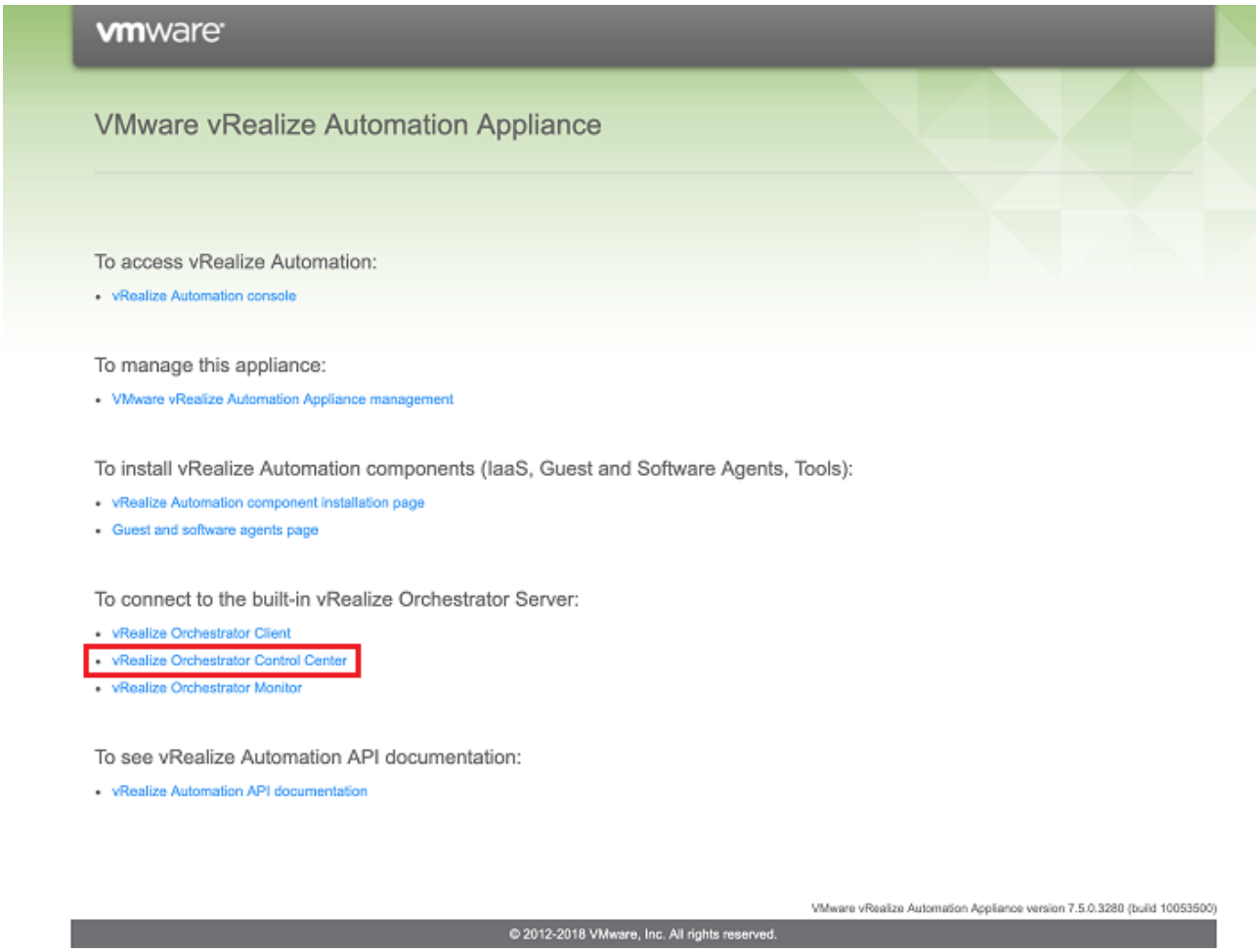
Installing the Plugin

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

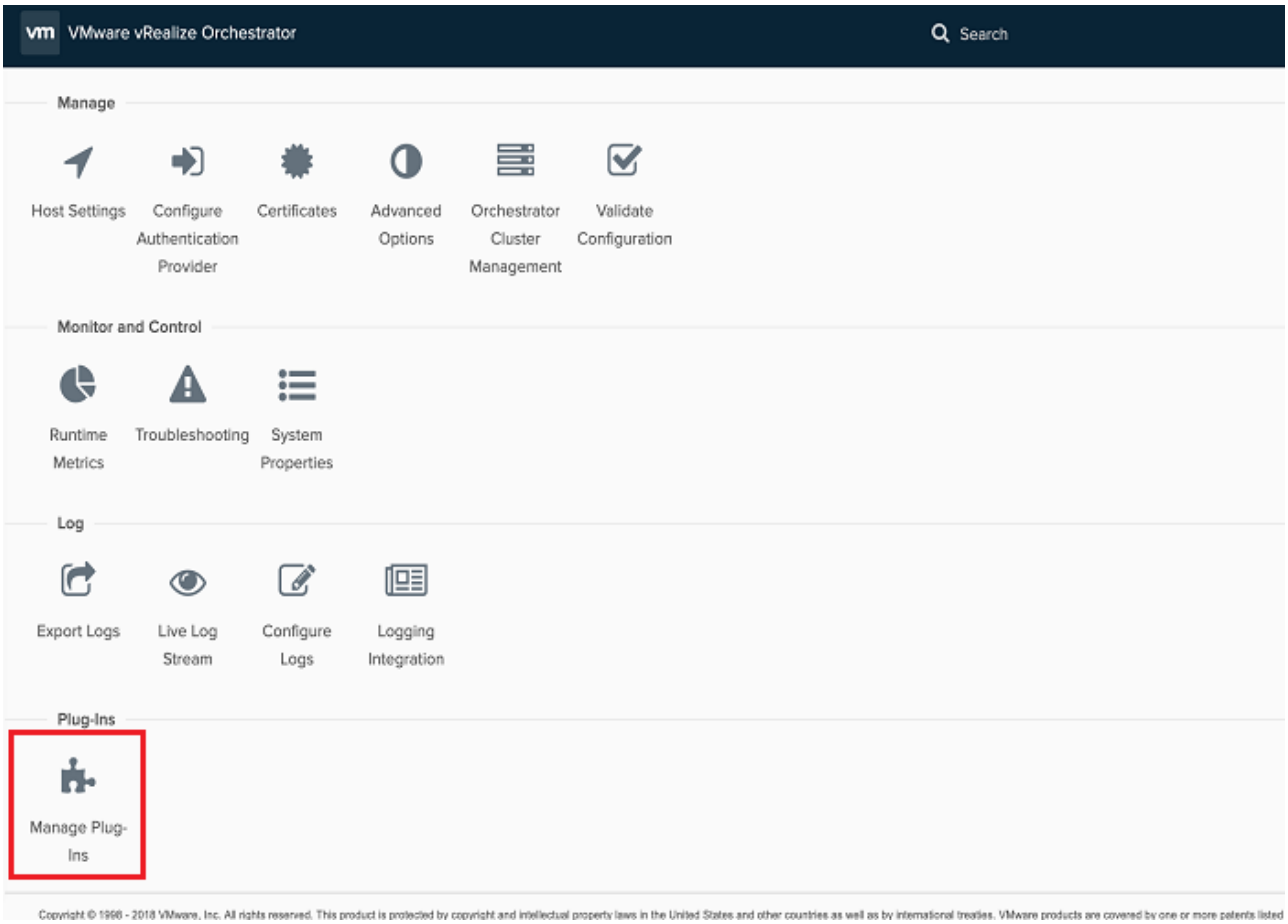
Note: If the Cohesity vRO plugin has already been installed and must be upgraded, you must first remove the existing plugin and then install the new Cohesity vRO plugin.

Procedure

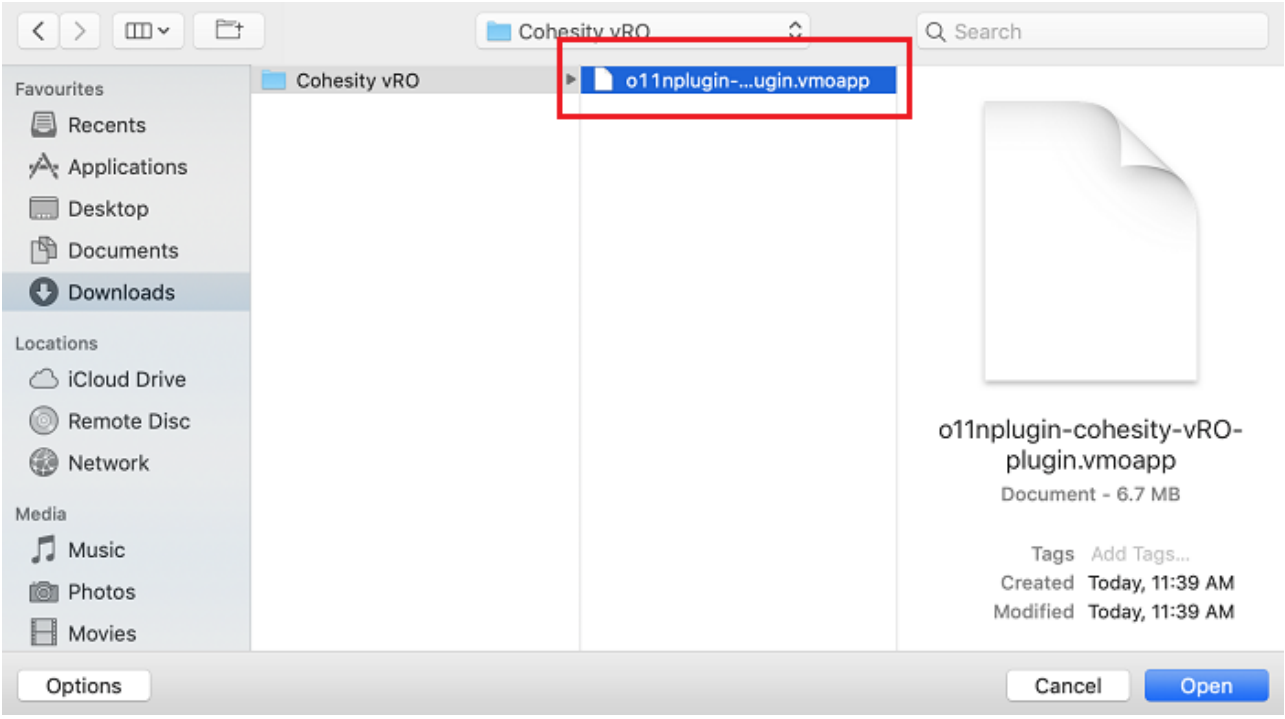
1. Login to the **vRealize Orchestrator** and click **vRealize Orchestrator Control Center**. You must know the credentials to log in to the Control Center.



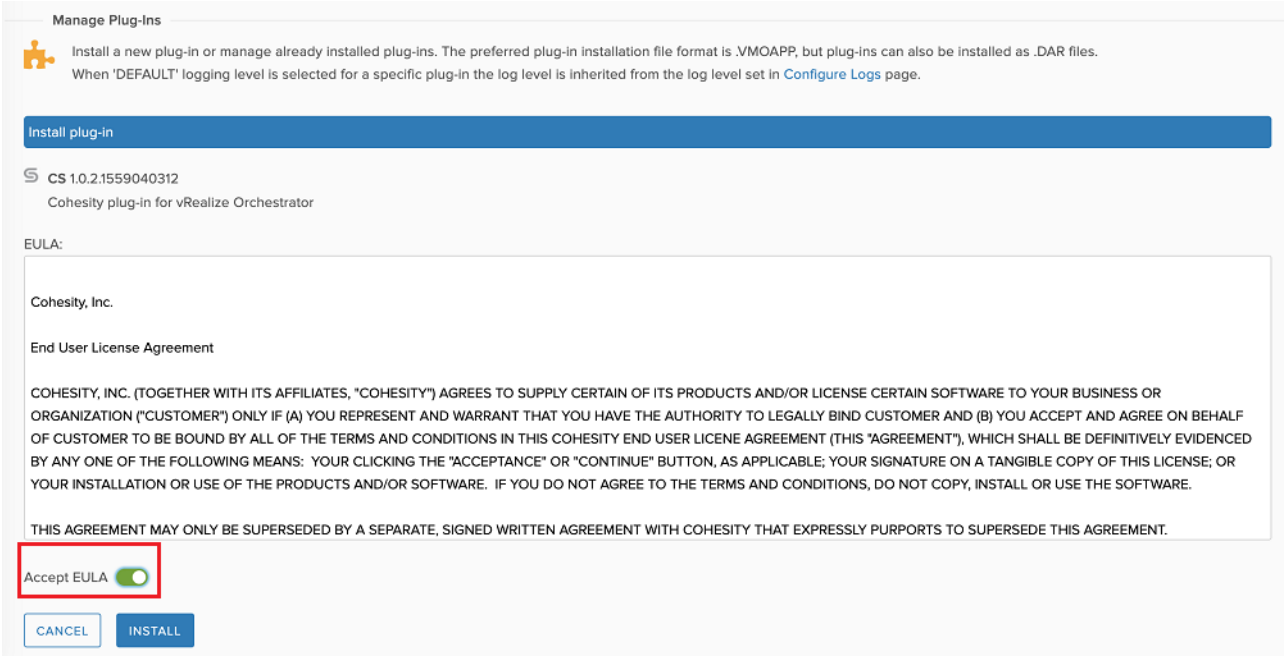
2. Click **Manage Plugins** in the displayed **vCenter Control Center** window.



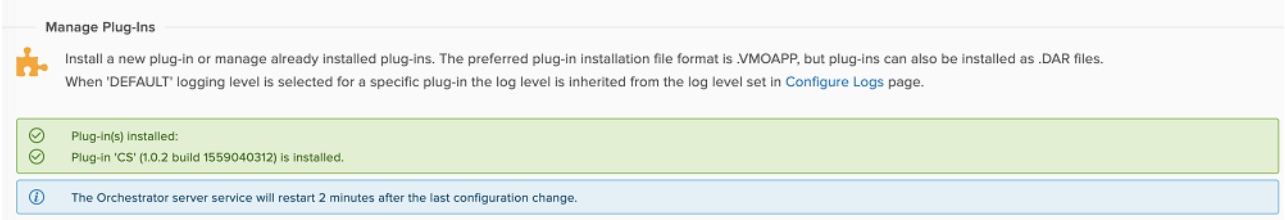
3. In the **Manage Plugins** section, click **Browse** to navigate to the folder where you have saved the ***.vmoapp*** file and select the source installer ***o11nplugin-cohesity-vRO-plugin.vmoapp/.dar.***



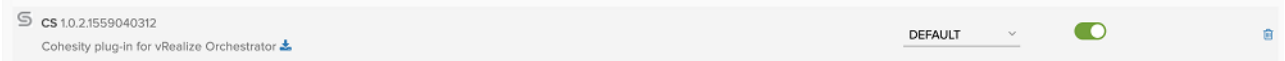
4. Click **Install**.
5. Read the end user license agreement and click **Accept EULA**.



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



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:



Removing the Plugin

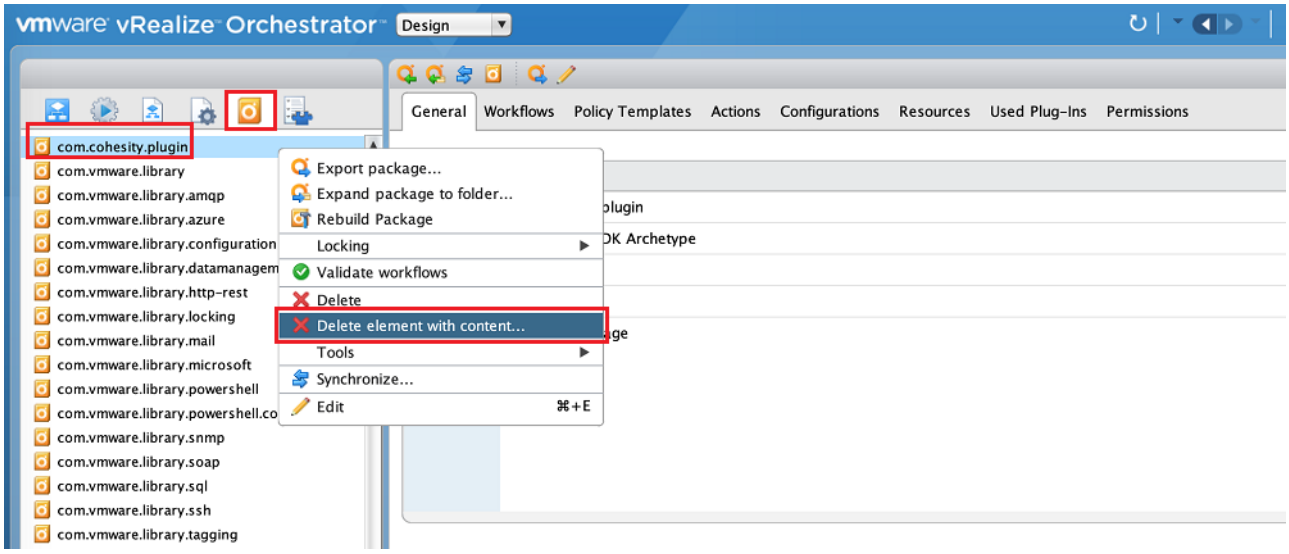
Procedure

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**.

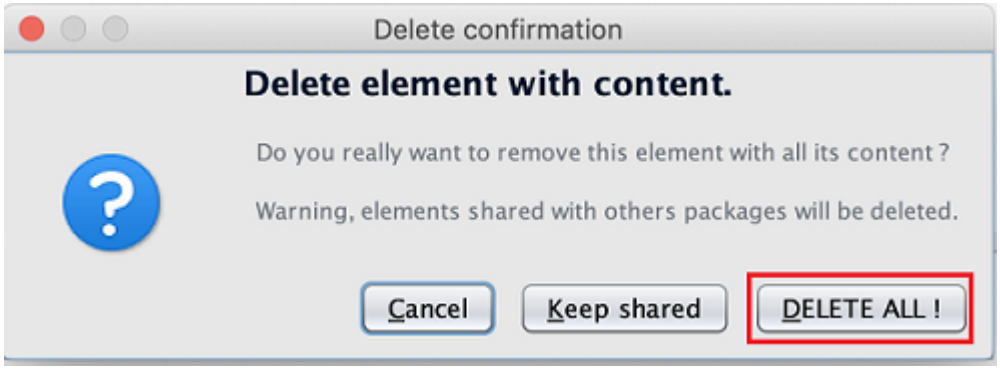
Alternatively, you can also click the **Remove** icon to remove the plugin.

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
Launching vRO Client	This section describes the basic steps to start the vRO Client.
Adding a Cohesity Endpoint	This section describes the details to add an endpoint and to connect vRO with the Cohesity Data Platform

Launching vRO Client

This section describes the basic steps to start the vRO clien

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-appliant-ip*.
2. Click on **vRealize Orchestrator** client.

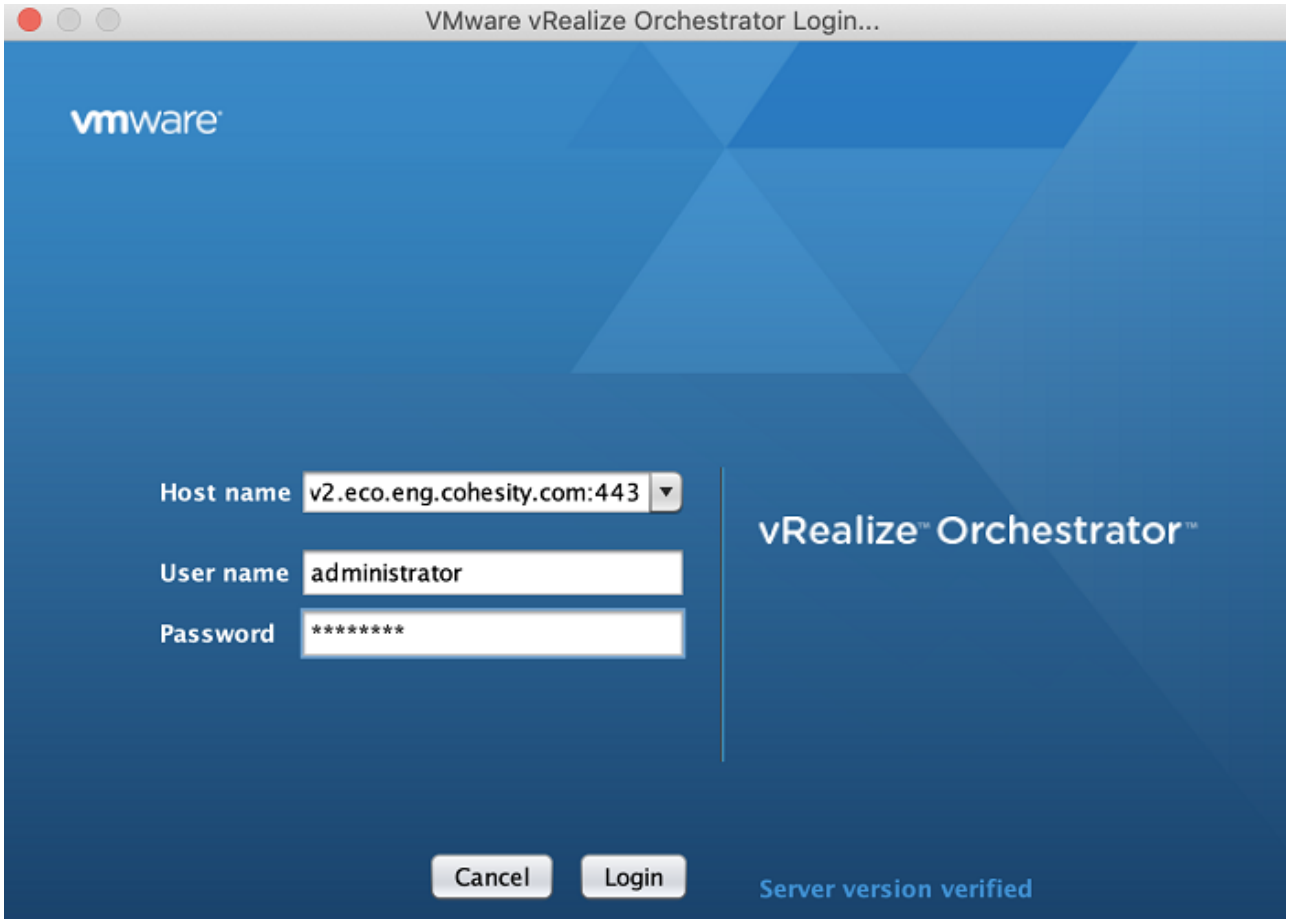
   A *client.jnlp* file is downloaded.
3. Open command prompt and run the following command.

   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.

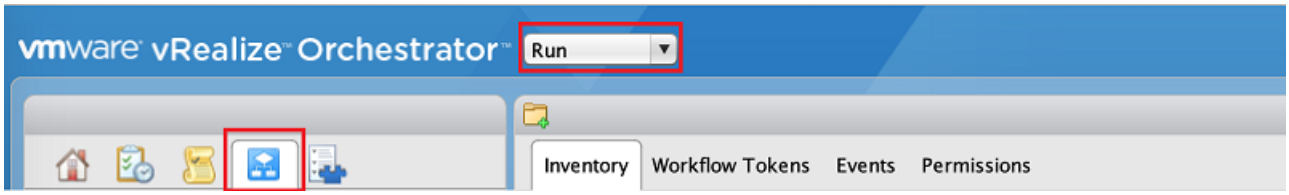
Procedure

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.

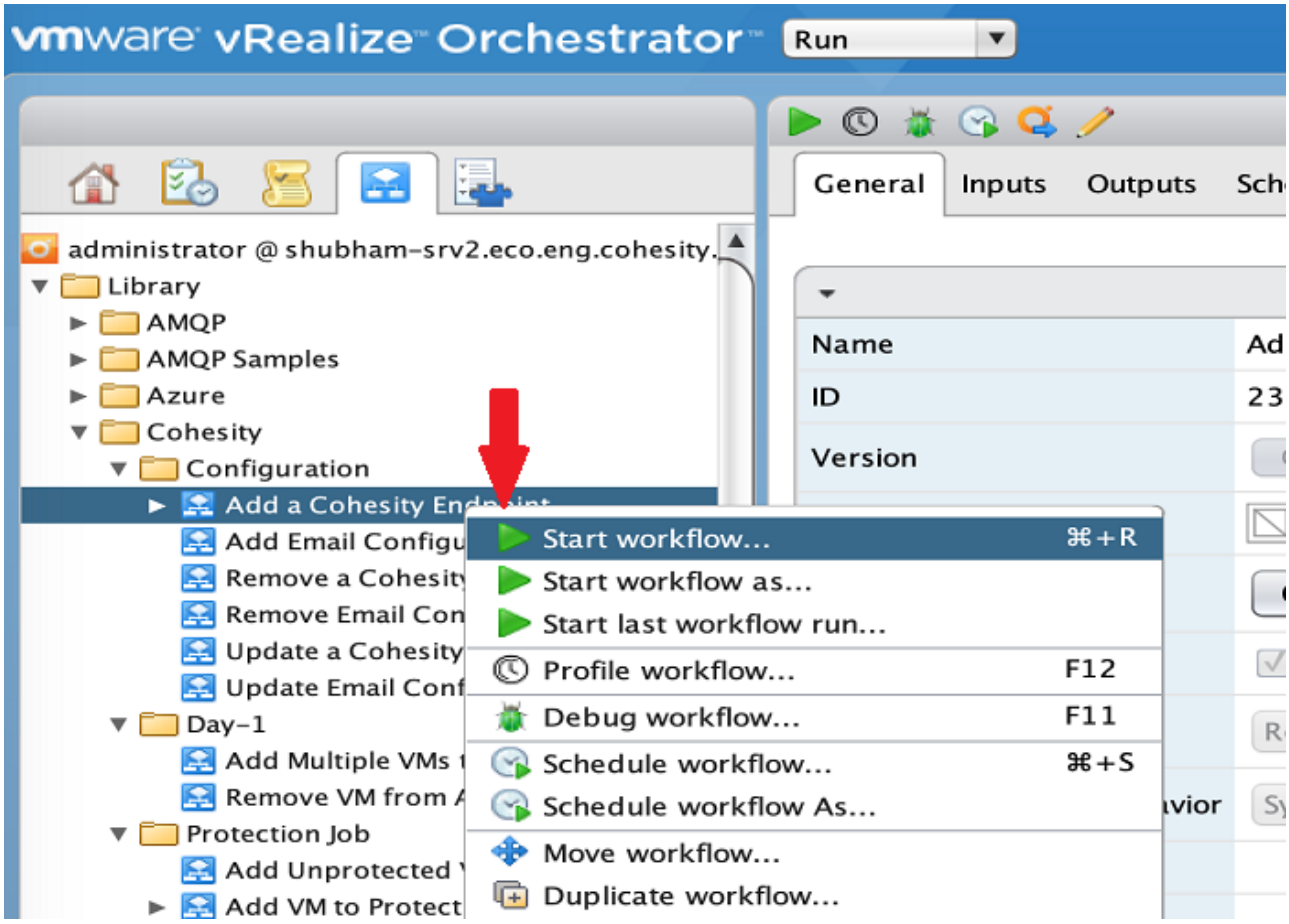
Adding a Cohesity Endpoint

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 **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.

Configuring vRA

In this Section

Topic	Description
Importing Blueprints	This section describes the details to import the XAAS blueprints.
Configuring Day 1 Workflows (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

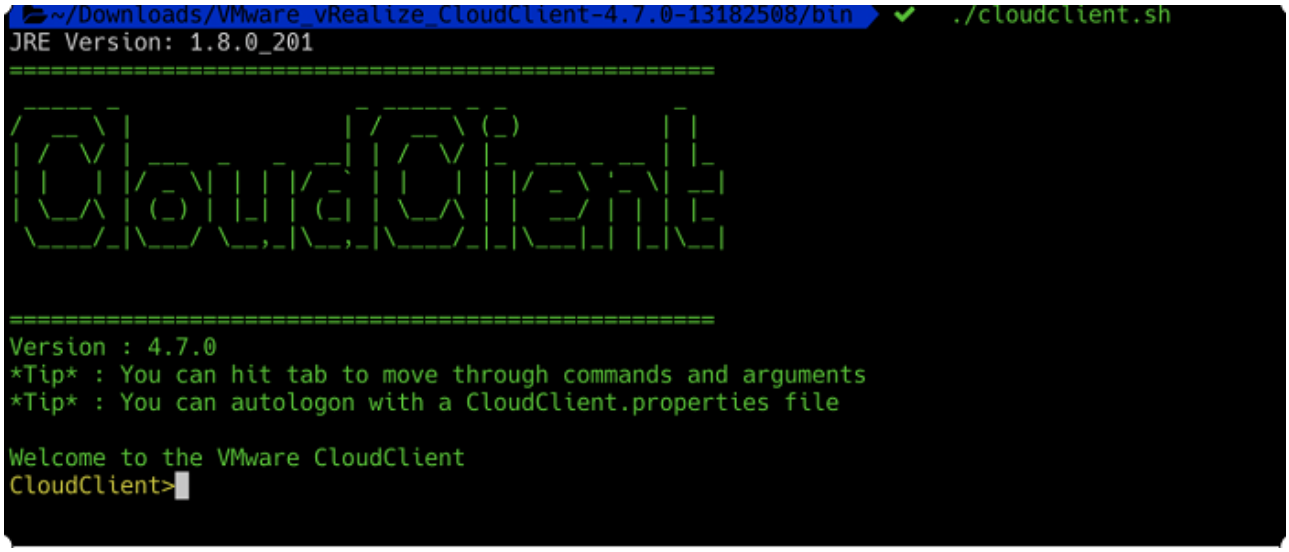
This section describes the details to import the XAAS blueprints.

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.

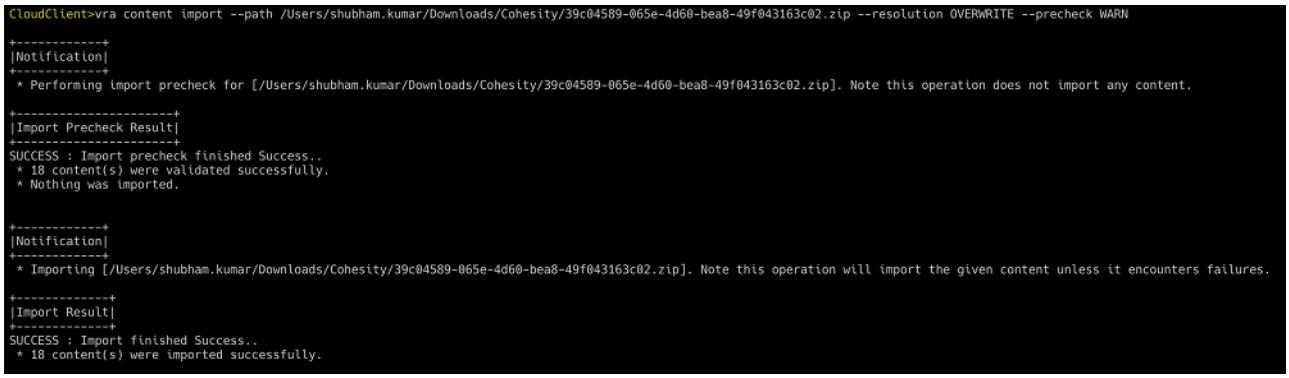
Procedure

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.



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>`

4. Import the blueprint file using the following command. `vra content import --path <path-to-zip-file> --resolution OVERWRITE --precheck WARN`



5. To verify if the import was successful, in VRA, navigate to **Design** > **XaaS** > **XaaS Blueprints** and check if all the Cohesity XASS workflows are available.

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

   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.

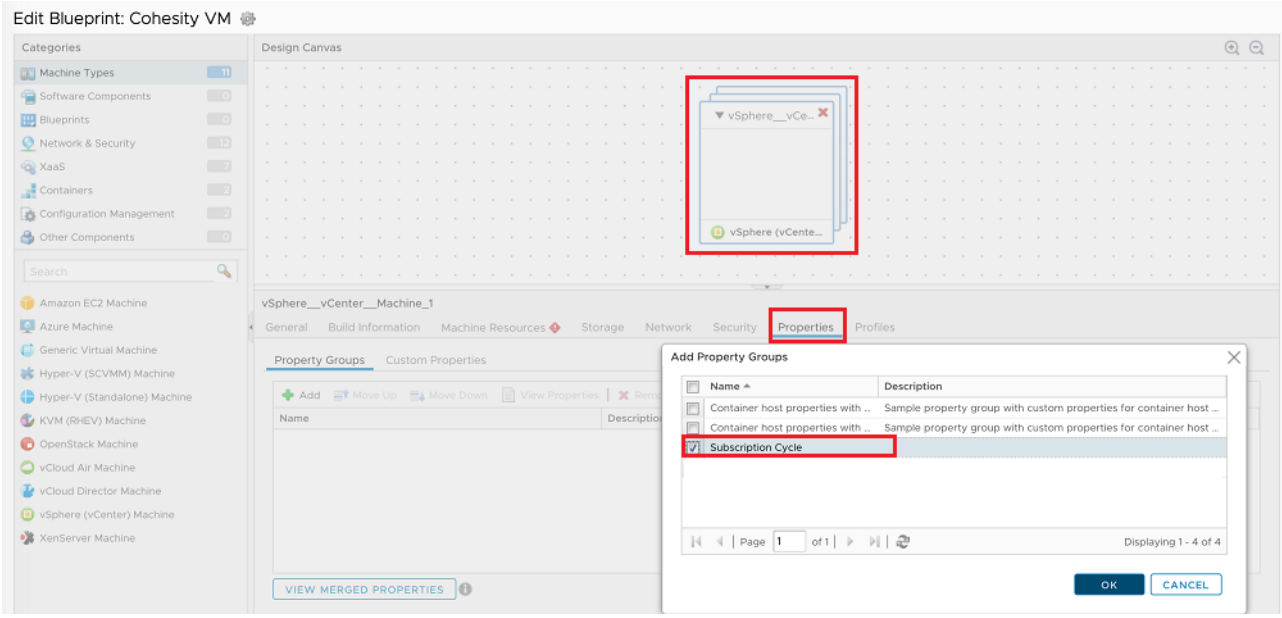
By configuring Day 1 Workflows, the VMs are added to the specified Protection Group when newly provisioned from VRA or removed from the protection group when the VM is destroyed.

Assigning Properties to Blueprint

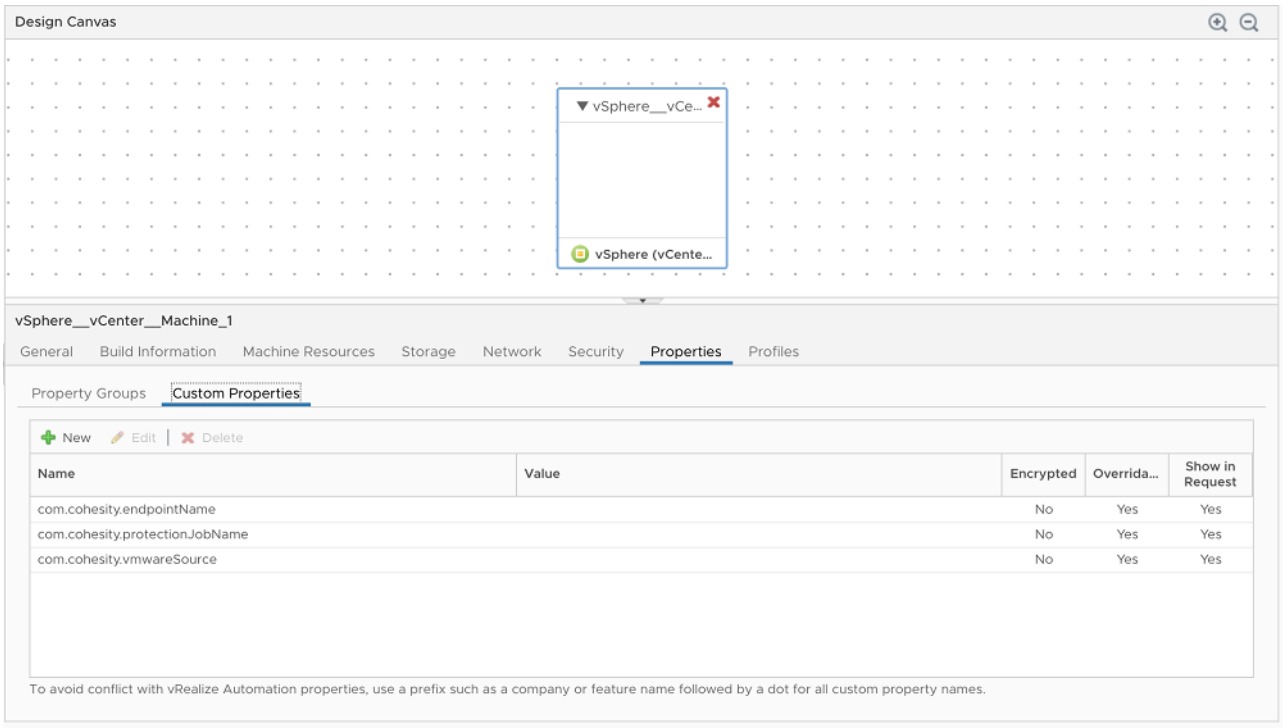
Procedure

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

1. In the **Design** tab, select **Blueprints**.
2. Select an existing blueprint from the **Blueprints** pane.
3. 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**.



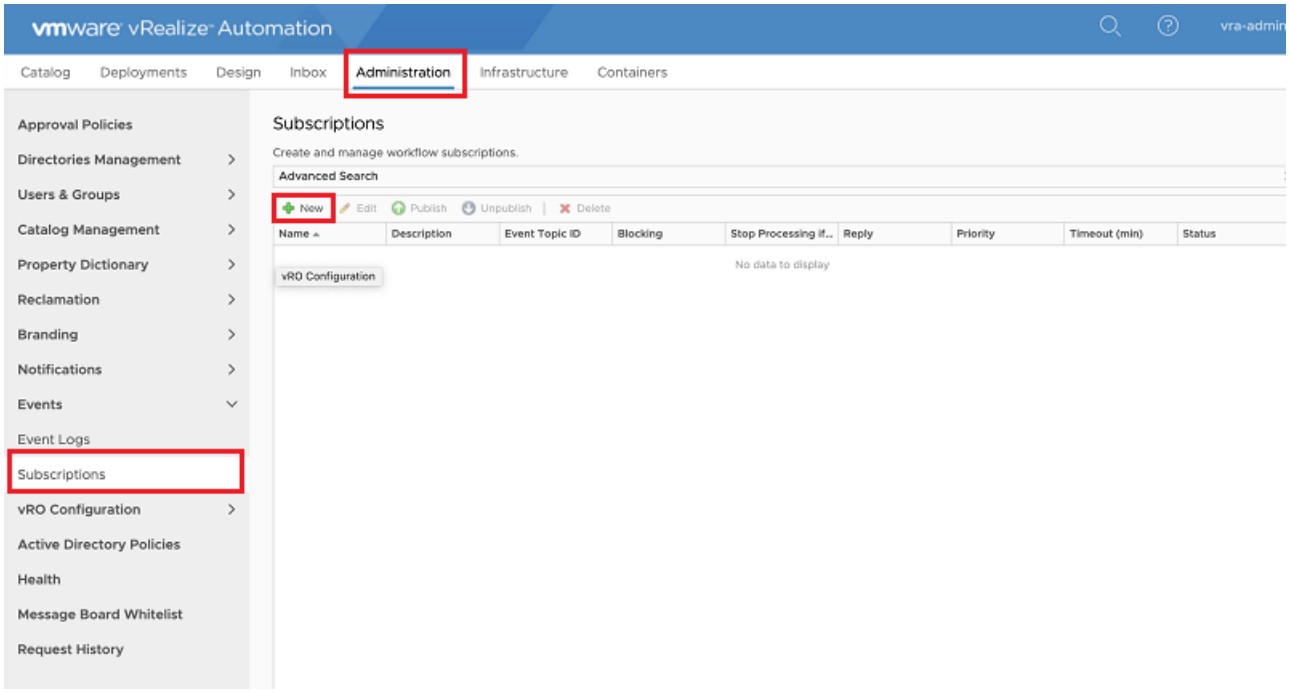
6. Click **SAVE** to save the changes.

Configuring Event Subscription

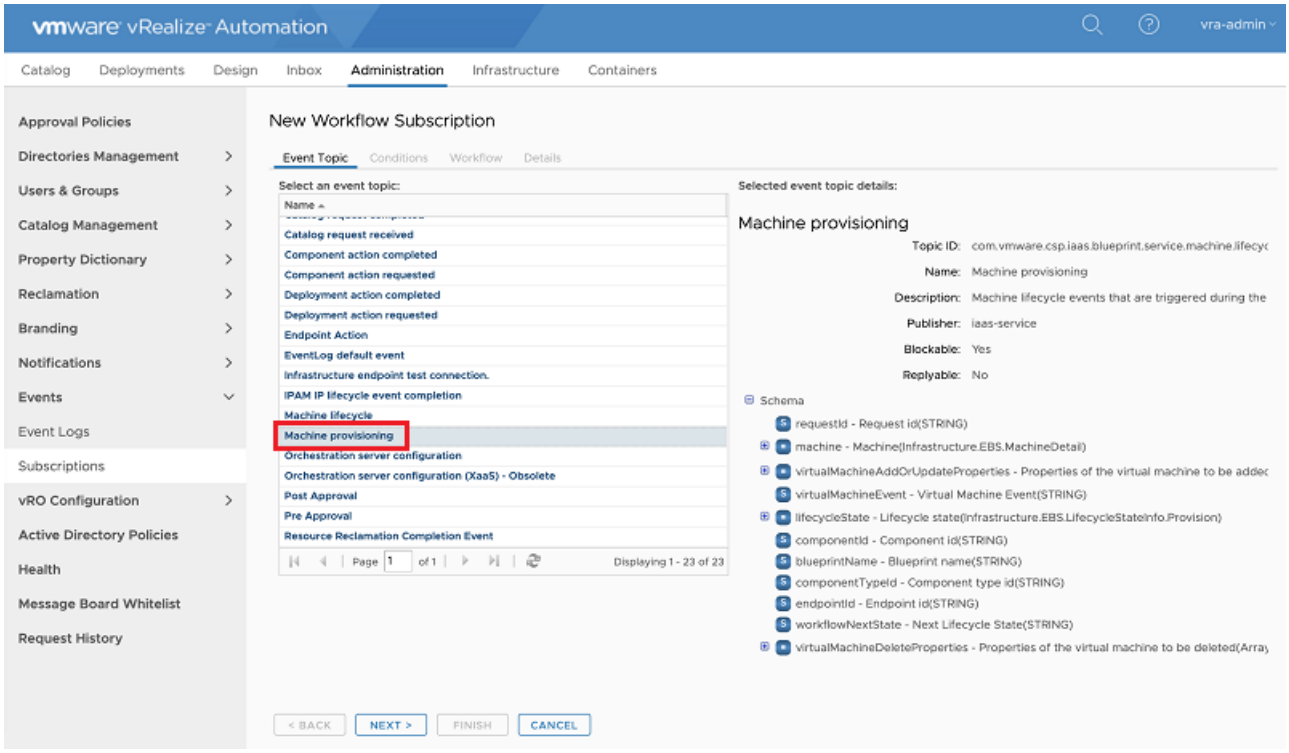
This section describes the steps you need to perform to create and configure event subscription.

Procedure

1. Click **Administration** > **Events** > **Subscriptions**.
2. To create a new workflow subscription, click the **New** icon.

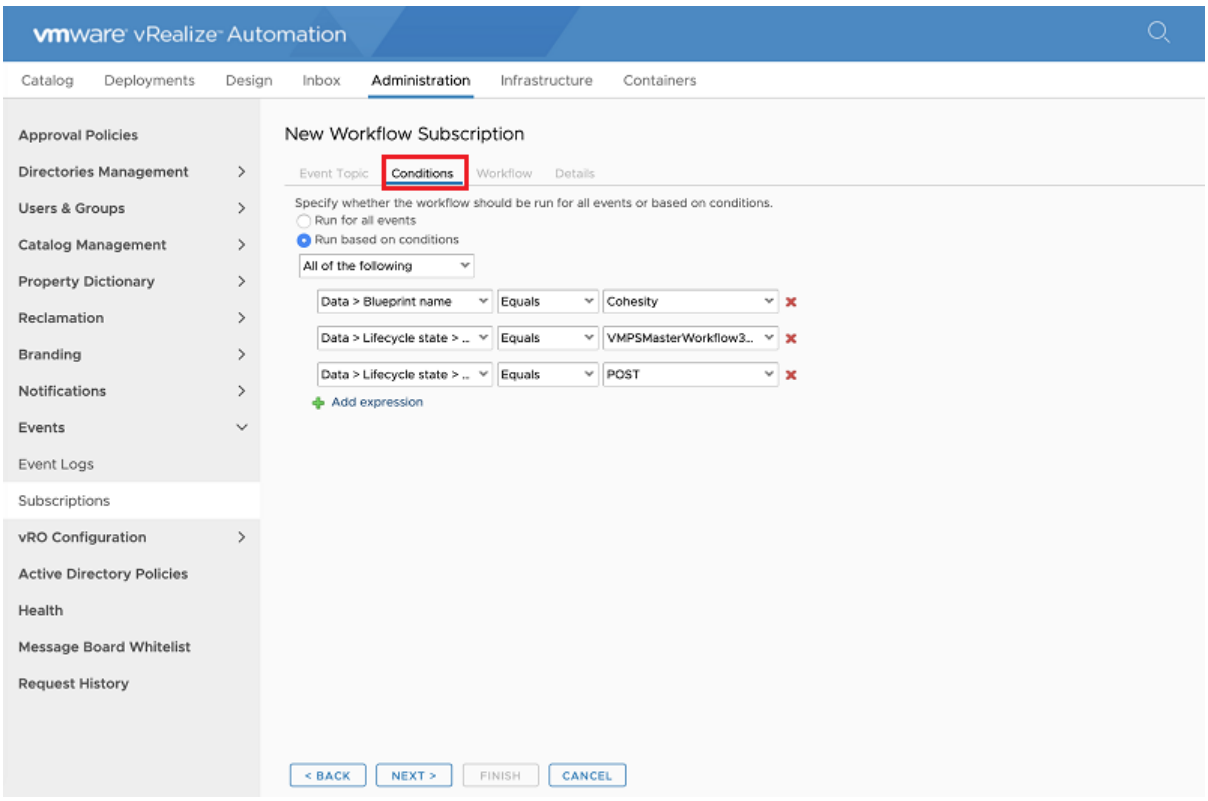


3. Select **Machine Provisioning** in the **Event Topic** page. Click **Next**.

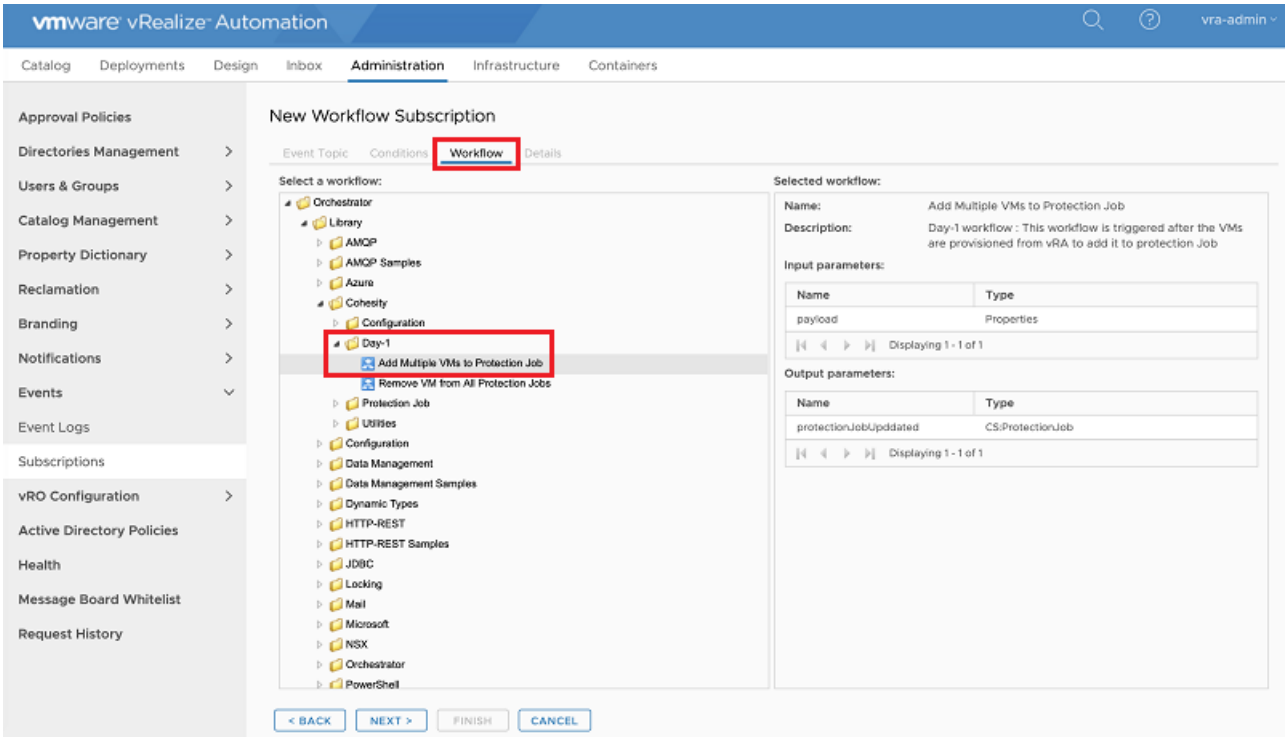


4. In the **Conditions** tab, select the following values and click **Next**.

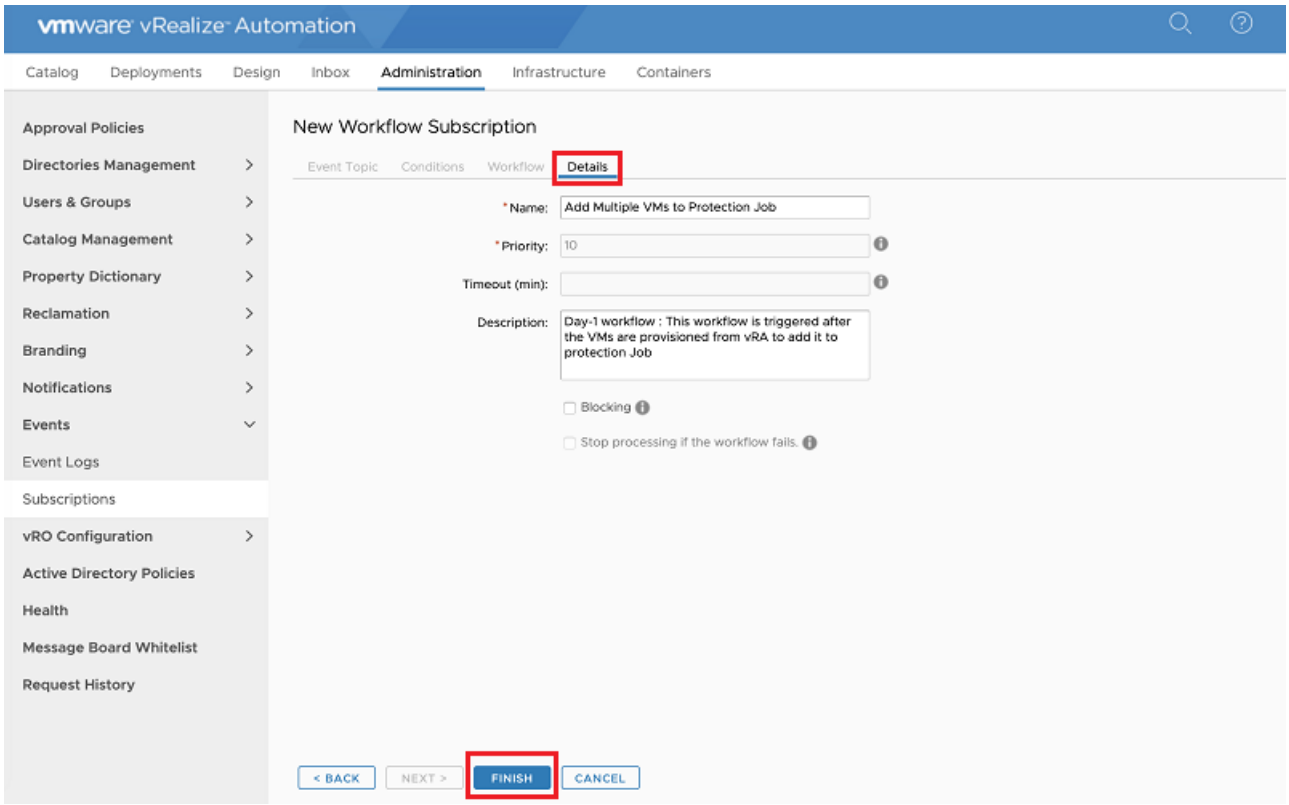
- *Run based on conditions = All of the following.*
- *Data > Blueprint Name = Cohesity (blueprint name to provision VM)*
- *Data > Lifecycle State >Lifecycle State Name = VMPSMasterWorkflow32.MachineProvisioned*
- *Data > Lifecycle State > State phase = POST*



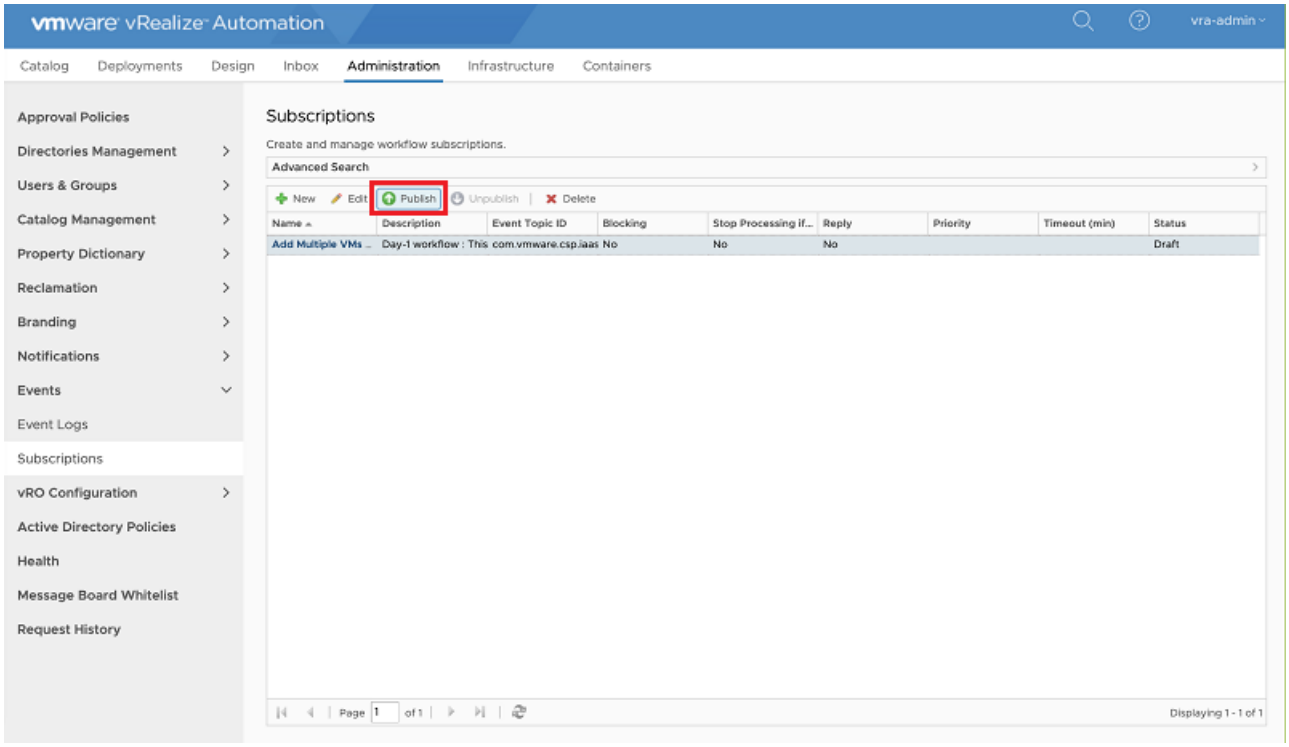
5. In the **Workflow** tab, select the workflow from Orchestrator and add this DAY-1 workflow of **Add Multiple VMs to Protection Group**.



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**.



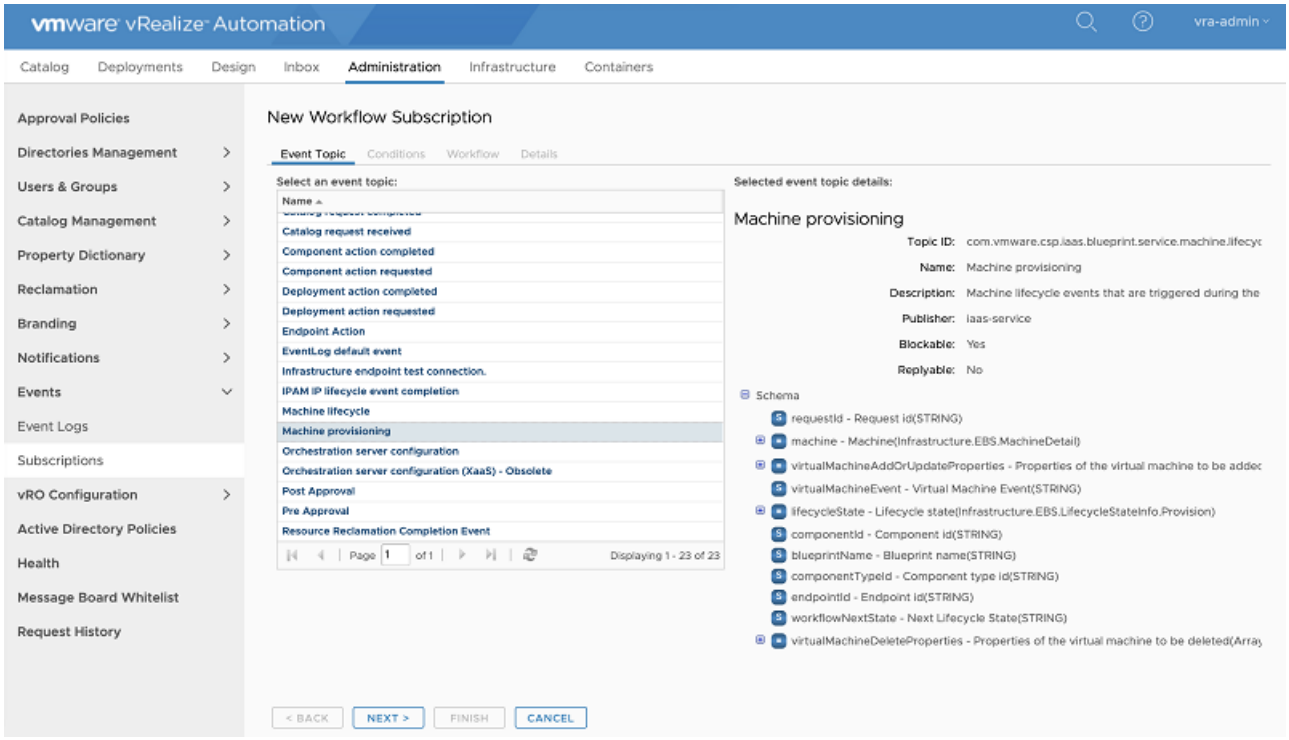
Remove VM from Protection Group

Procedure

To remove VM from Protection Group when VM is destroyed:

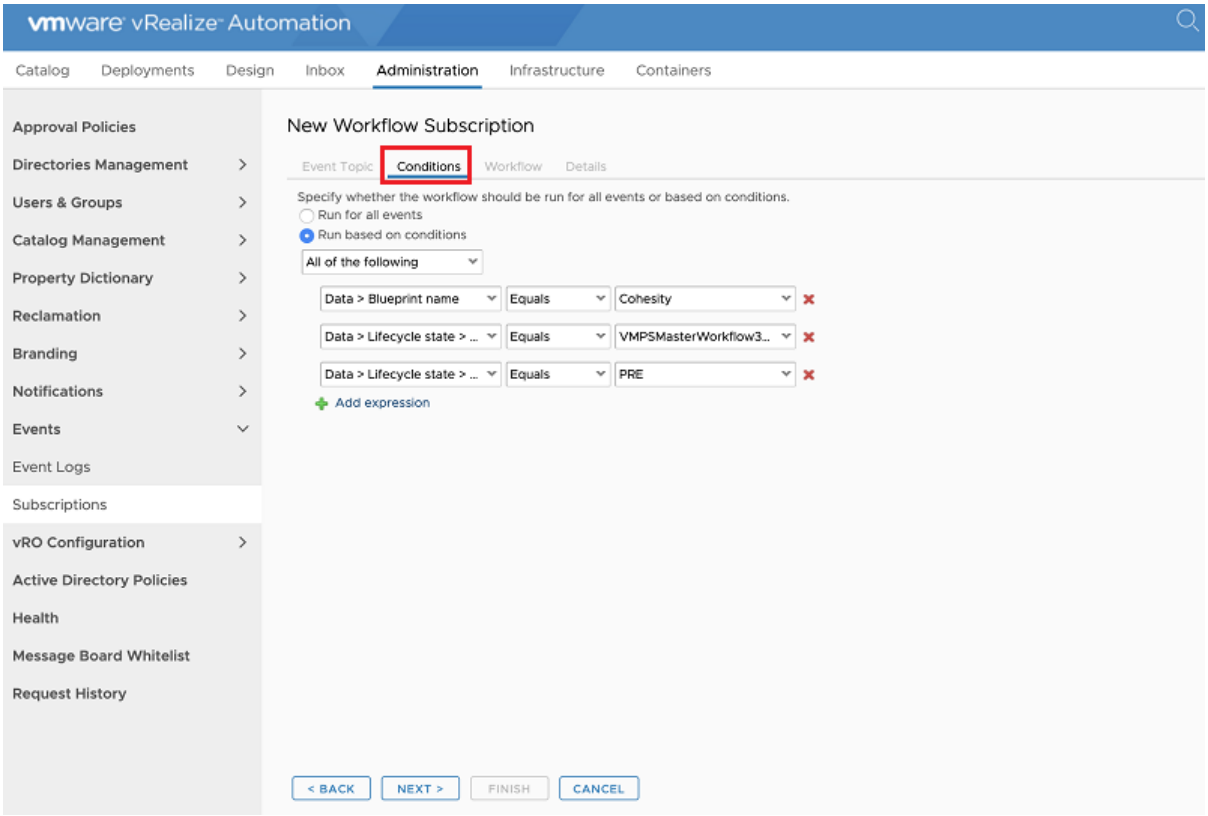
1. Click **Administration** > **Events** > **Subscriptions**.

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

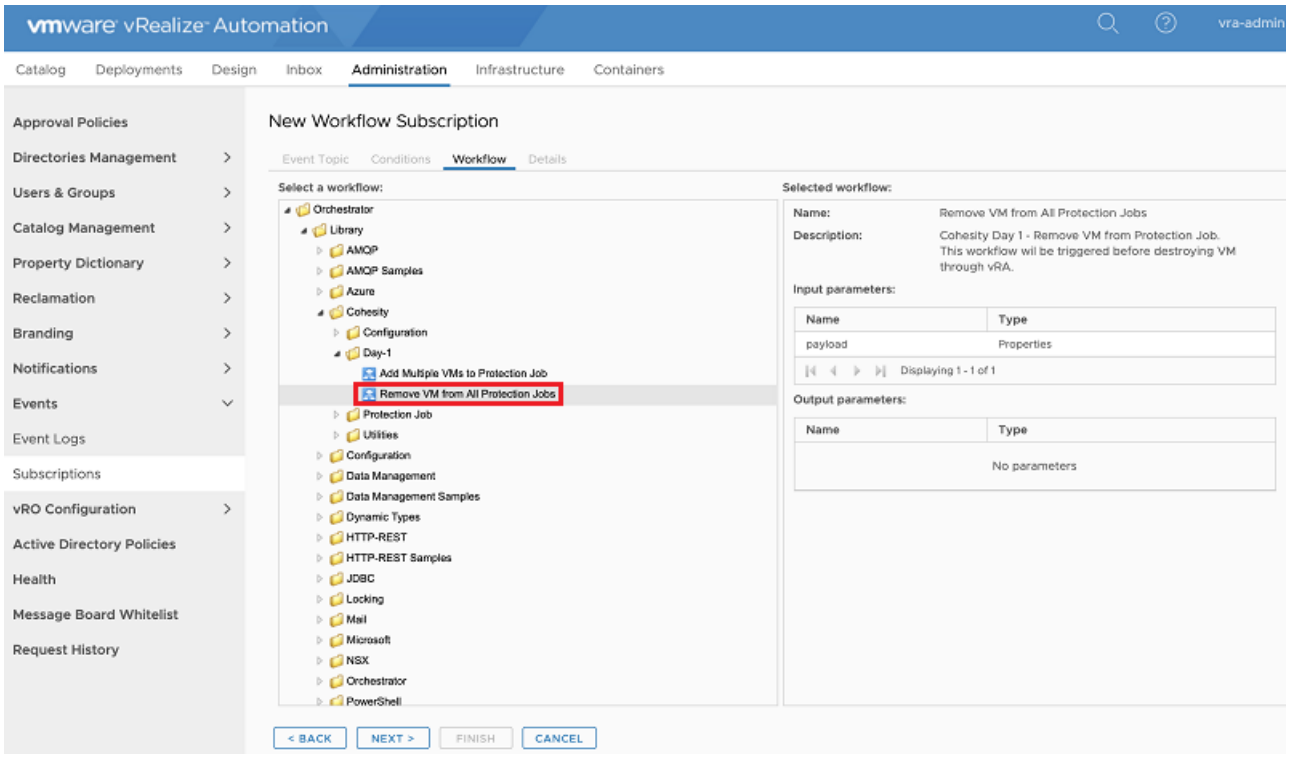


3. In the **Conditions** tab, select the following and click **Next**.

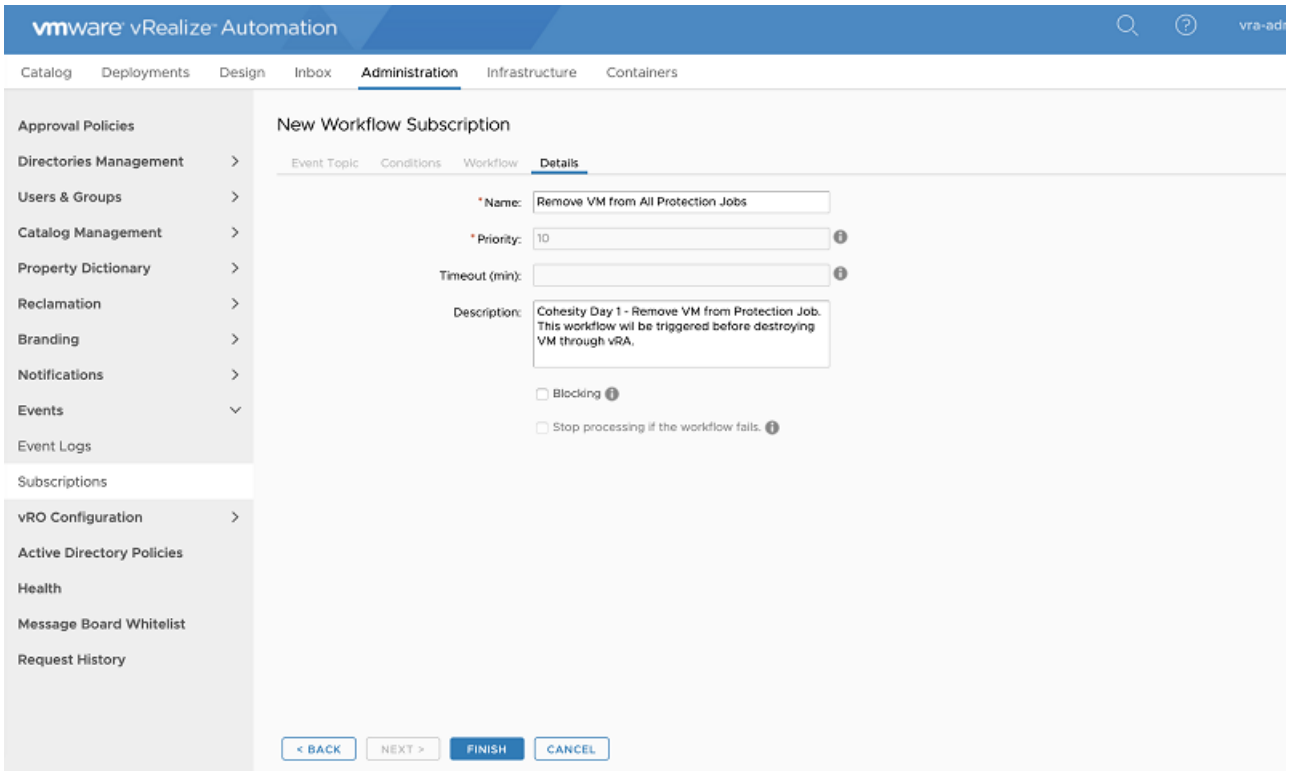
   - *Run based on conditions = All of the following.*
   - *Data > Blueprint Name = Cohesity (BluePrint name to the provision VM)*
   - *Data > Lifecycle State >Lifecycle State Name = VMPSMasterWorkflow32.UnprovisionMachine*
   - *Data > Lifecycle State > State phase = PRE*



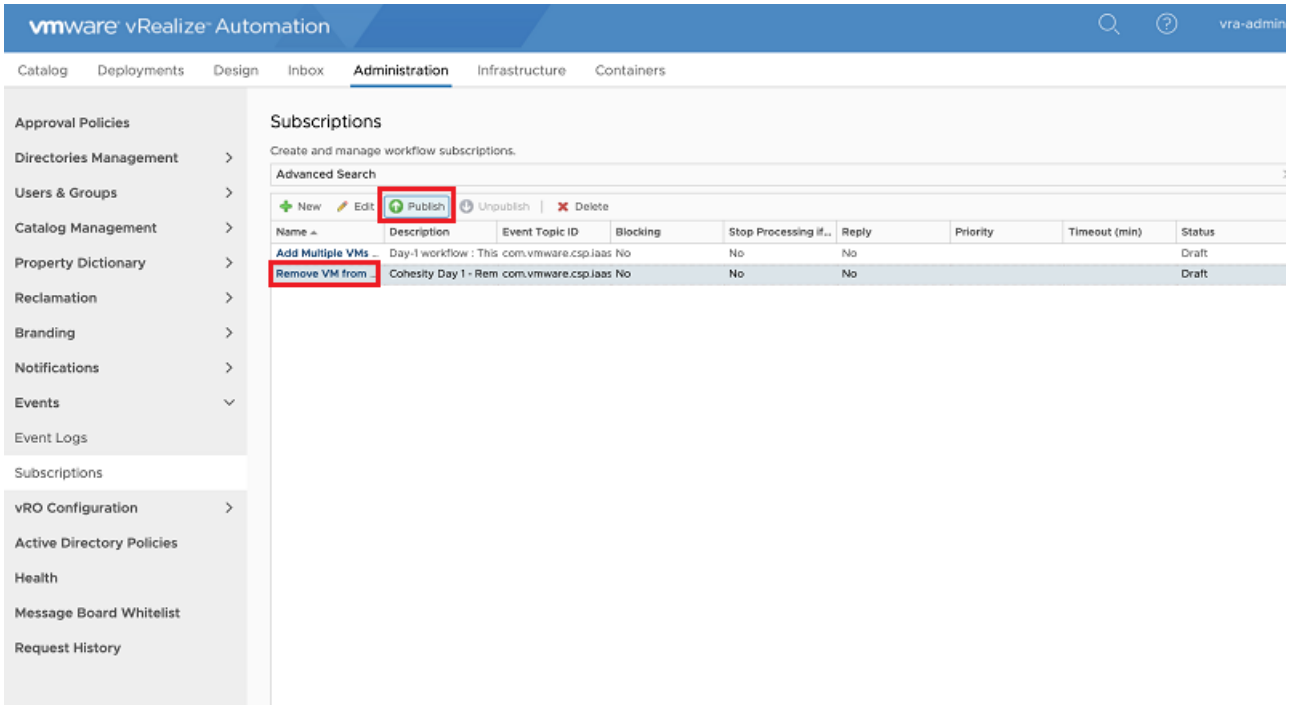
4. Select the workflow from Orchestrator and select the **DAY-1** workflow of **Remove VM from All Protection Groups** in this page.



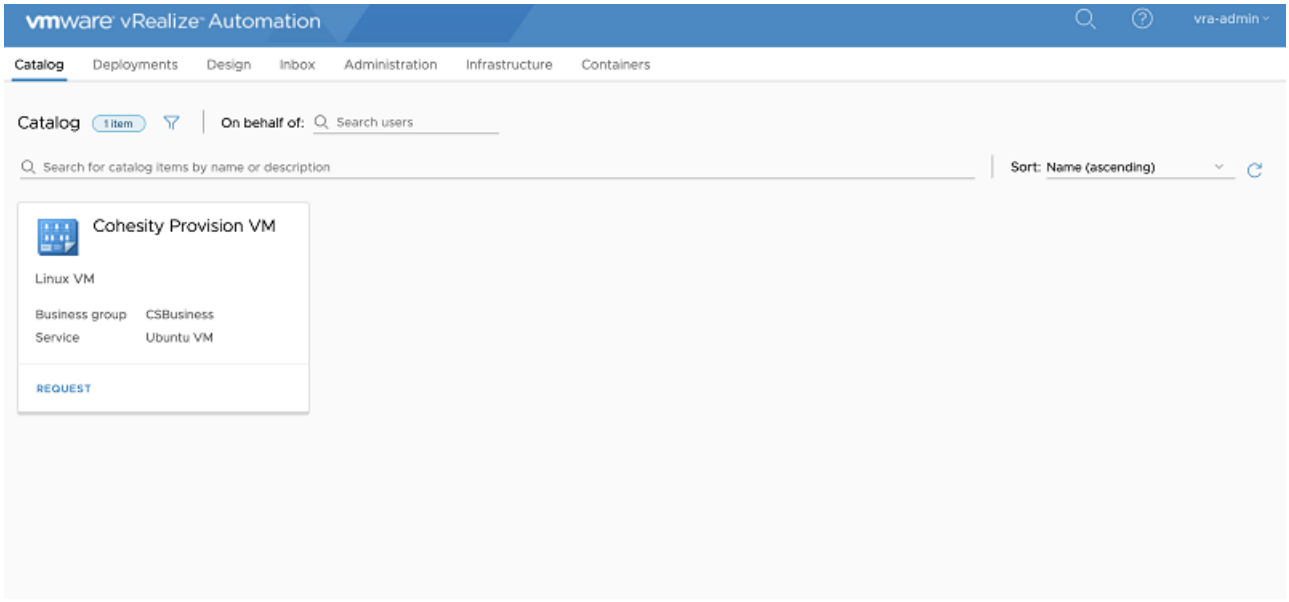
5. In the **Details** tab, enter the new **Subscription Name** (It will use the Workflow name by default) and then click **Finish**.



6. Select the newly created subscription and publish it.



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.



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

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

Note: The steps to execute a Protection Group 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.

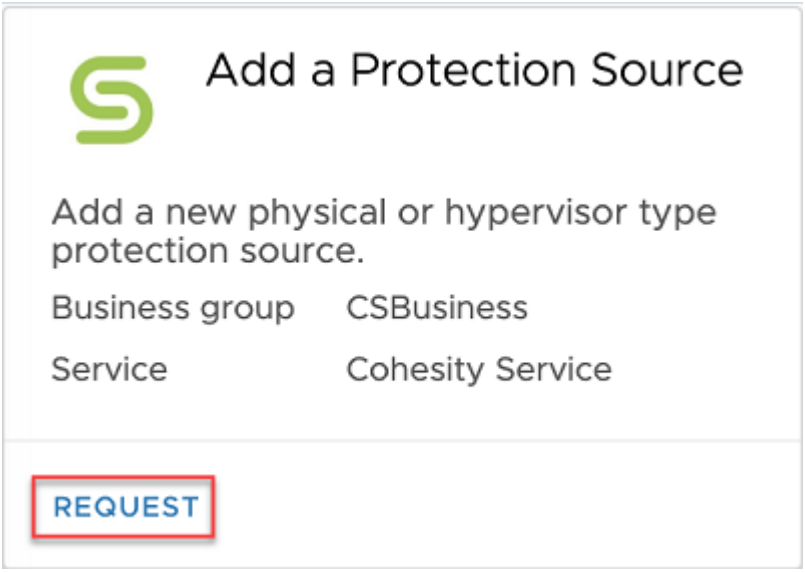
Adding a Protection Source

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**.

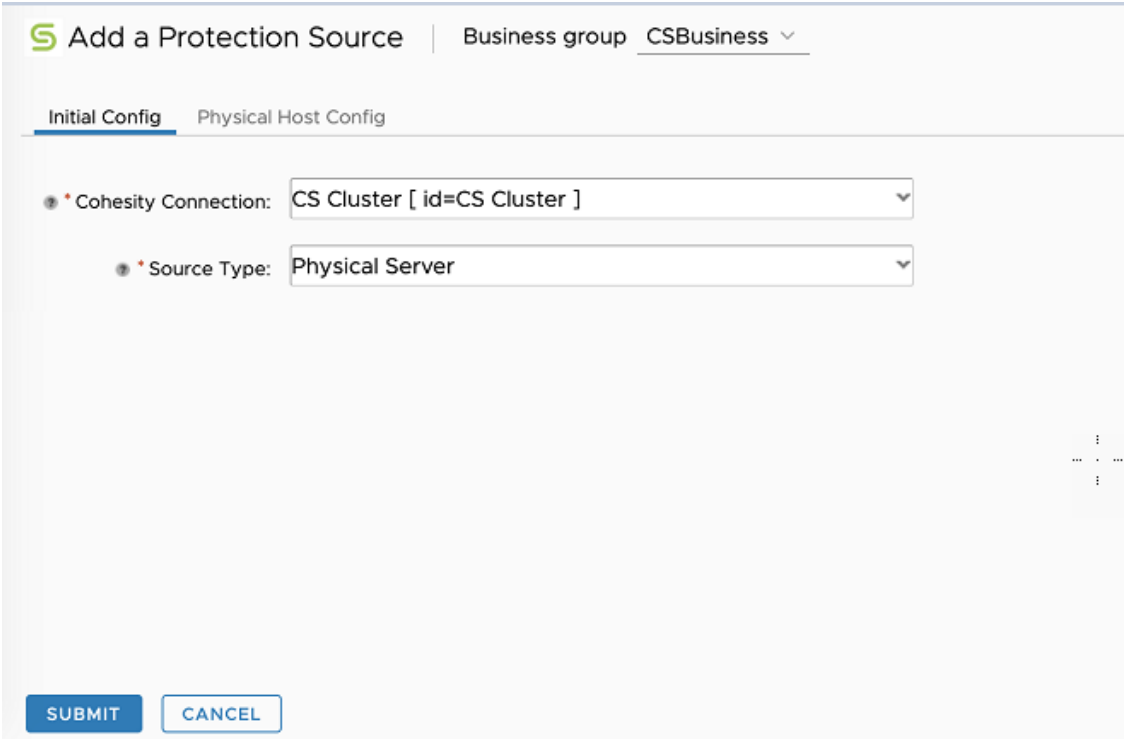
2. Click **REQUEST** on **Add a Protection Source**.



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

    - Physical Server:

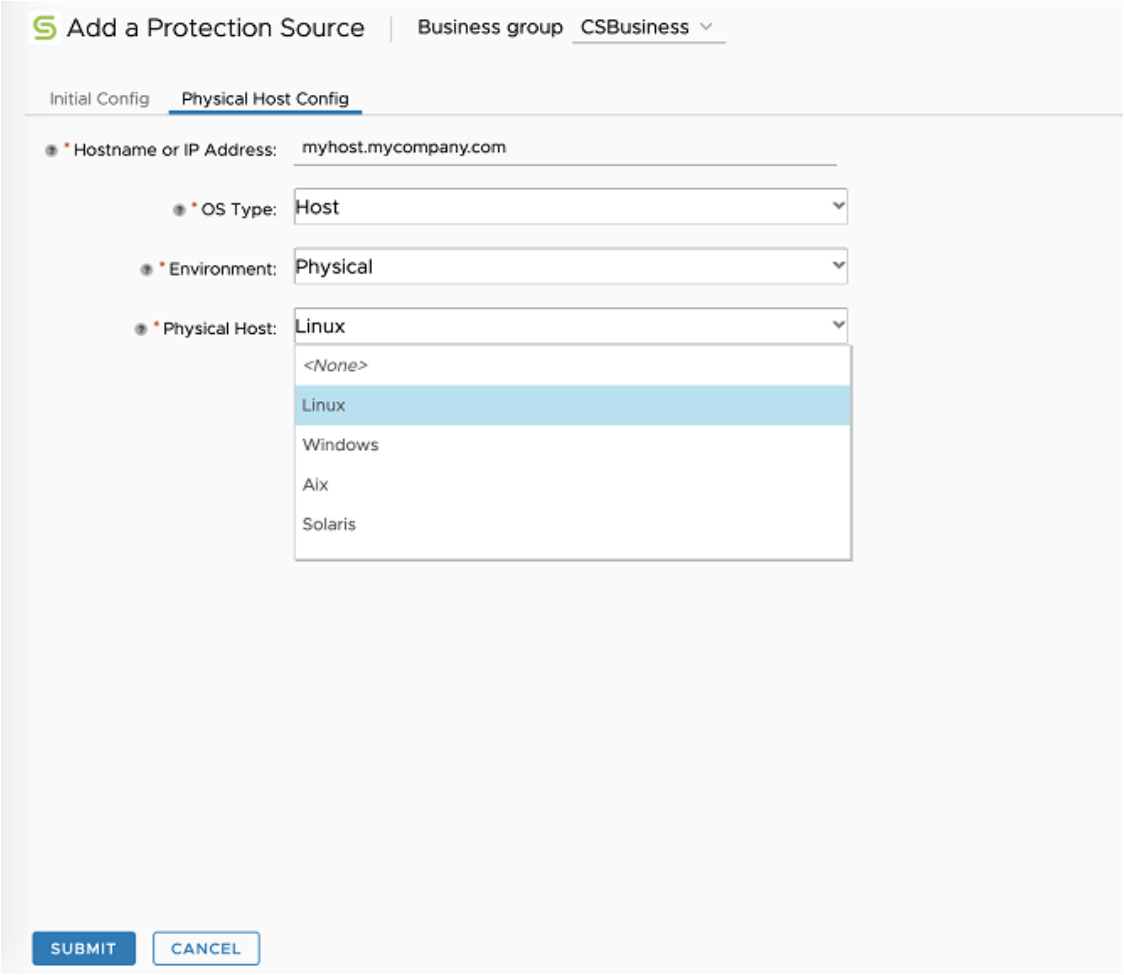
        1. On selecting a **Physical Server**, a new tab called **Physical Host Config** is displayed.



        2. Specify the following details:

Parameter	Description

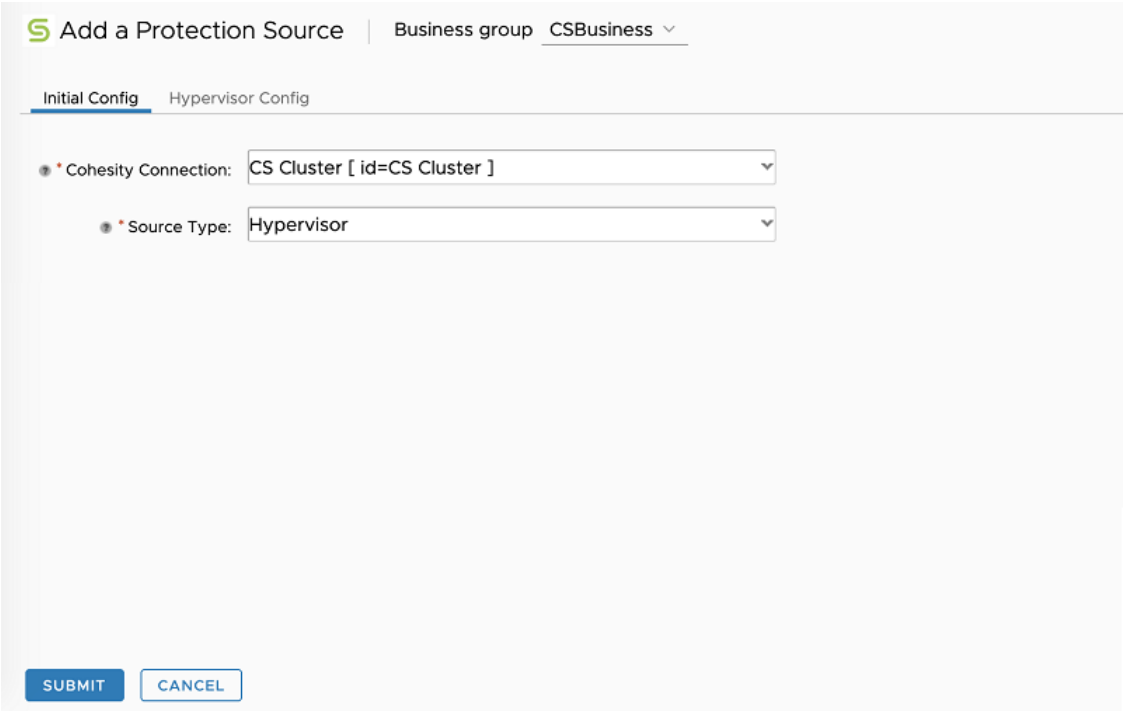
Parameter	Description
Hostname or IP Address	Enter the hostname or the IP address of the physical machine. Note: Ensure that Cohesity agent is installed on this machine.
OS Type	Select the appropriate OS type as Host or WindowsCluster. By default, Host is selected.
Environment	Select the environment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



3. Click **Submit**.

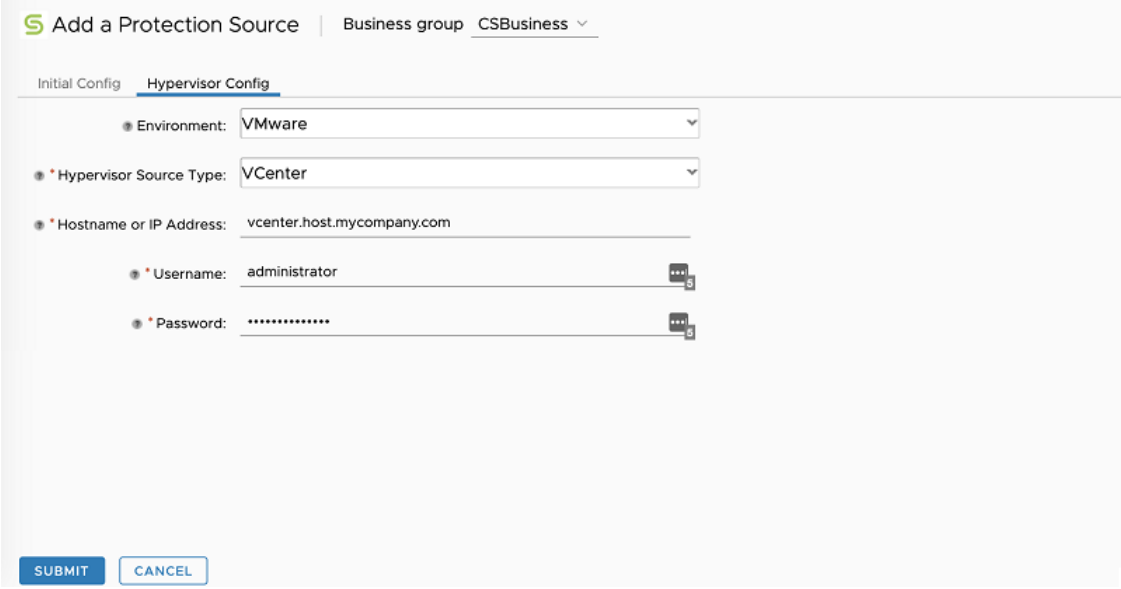
- Hypervisor:

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



2. Specify the following details:

Parameter	Description
Environment	Select the environment to be a VMware or a HyperV.
Hypervisor Source Type	This option is displayed **only** if the environment is *VMware*. 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.



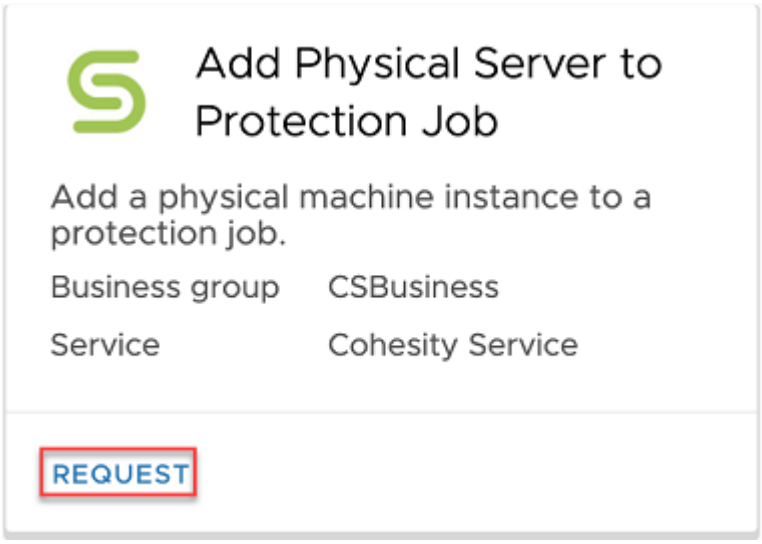
3. Click **Submit**.

Adding Physical Server to Protection Group

Procedure (XAAS)

To add a physical machine instance to a Protection Group:

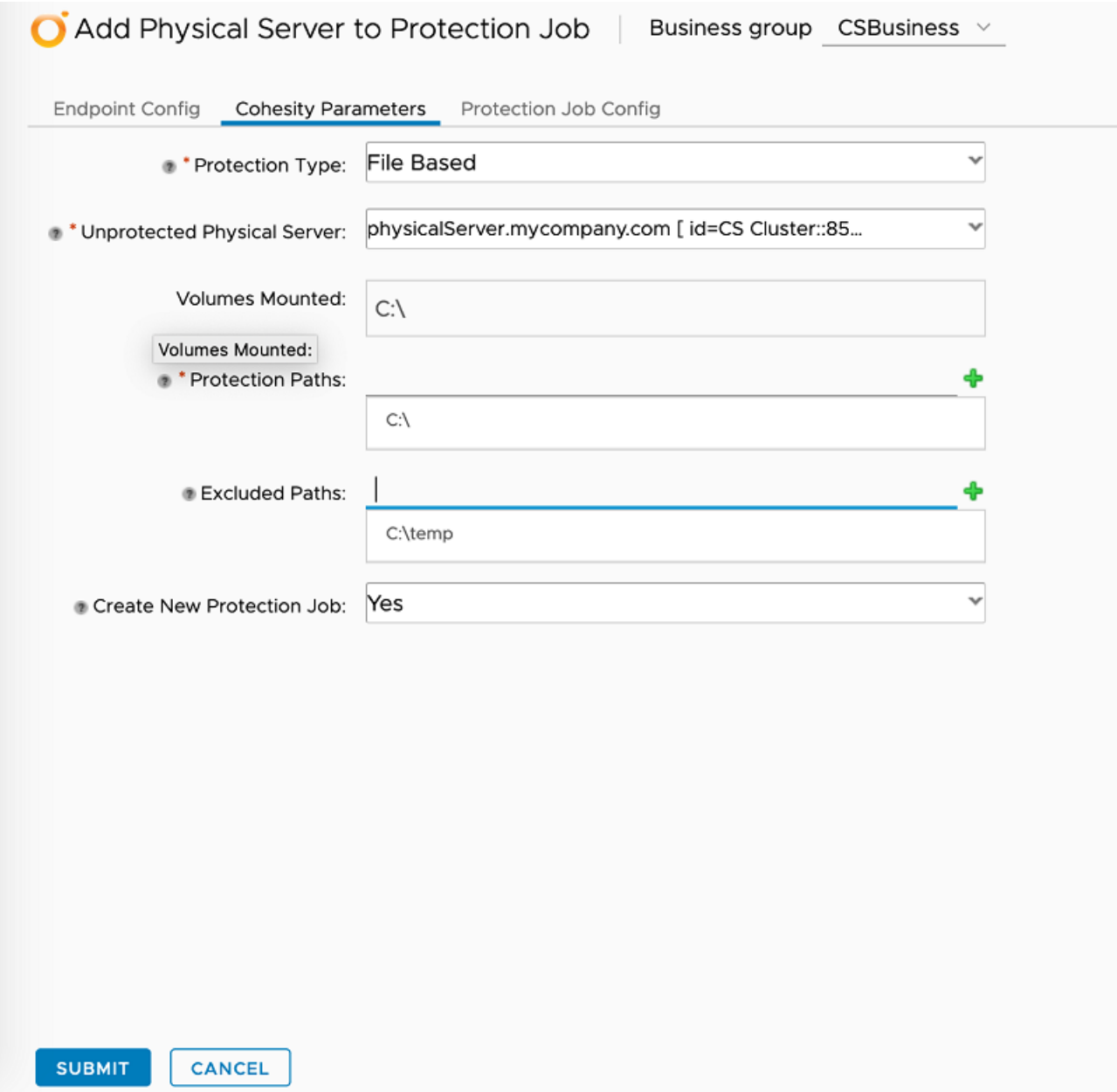
1. In the Catalog Dashboard, click **REQUEST** on **Add Physical Server to Protection Group**.



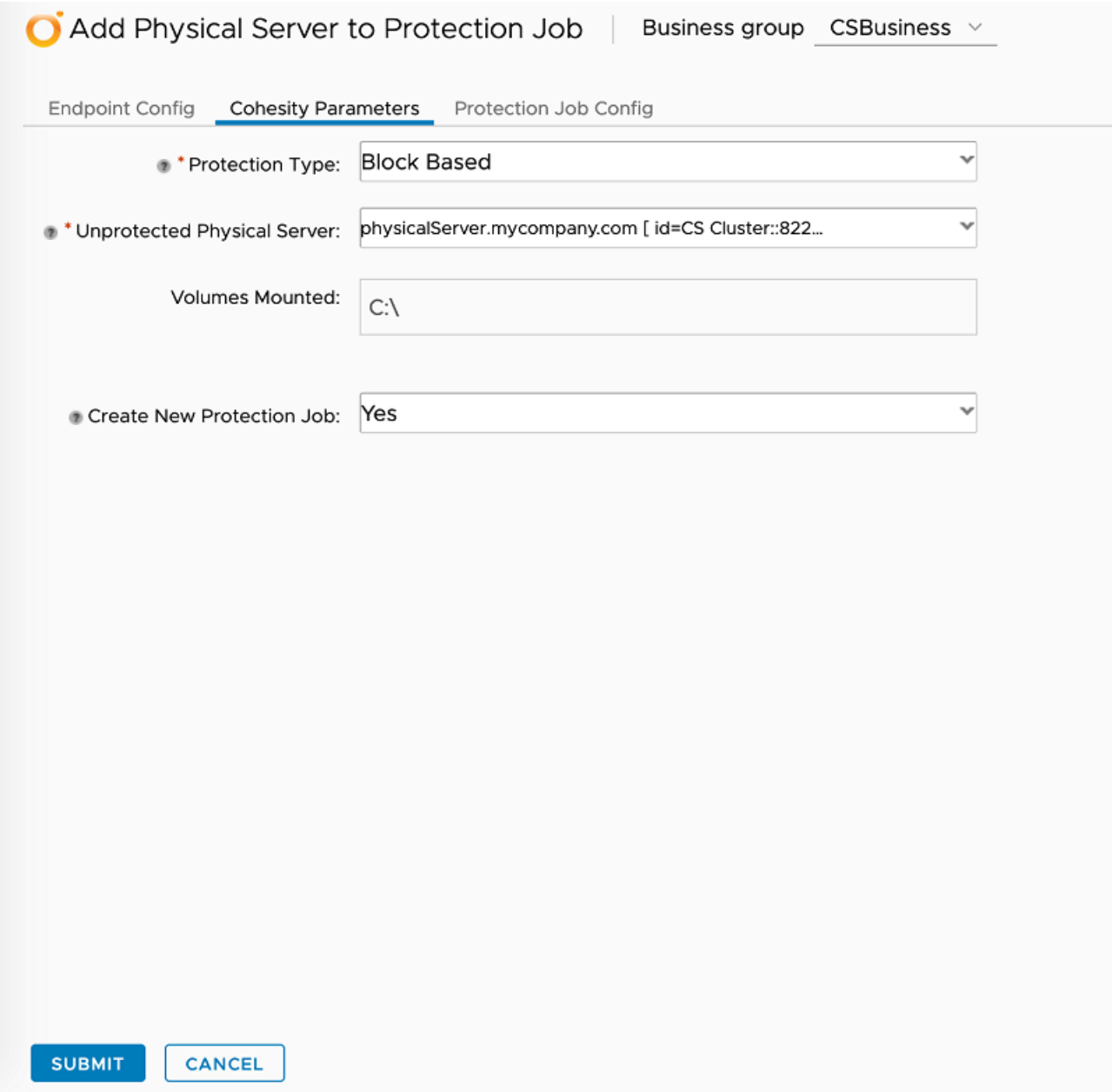
2. Select the **Cohesity Endpoint** from the drop down list. and click **Submit**.

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:



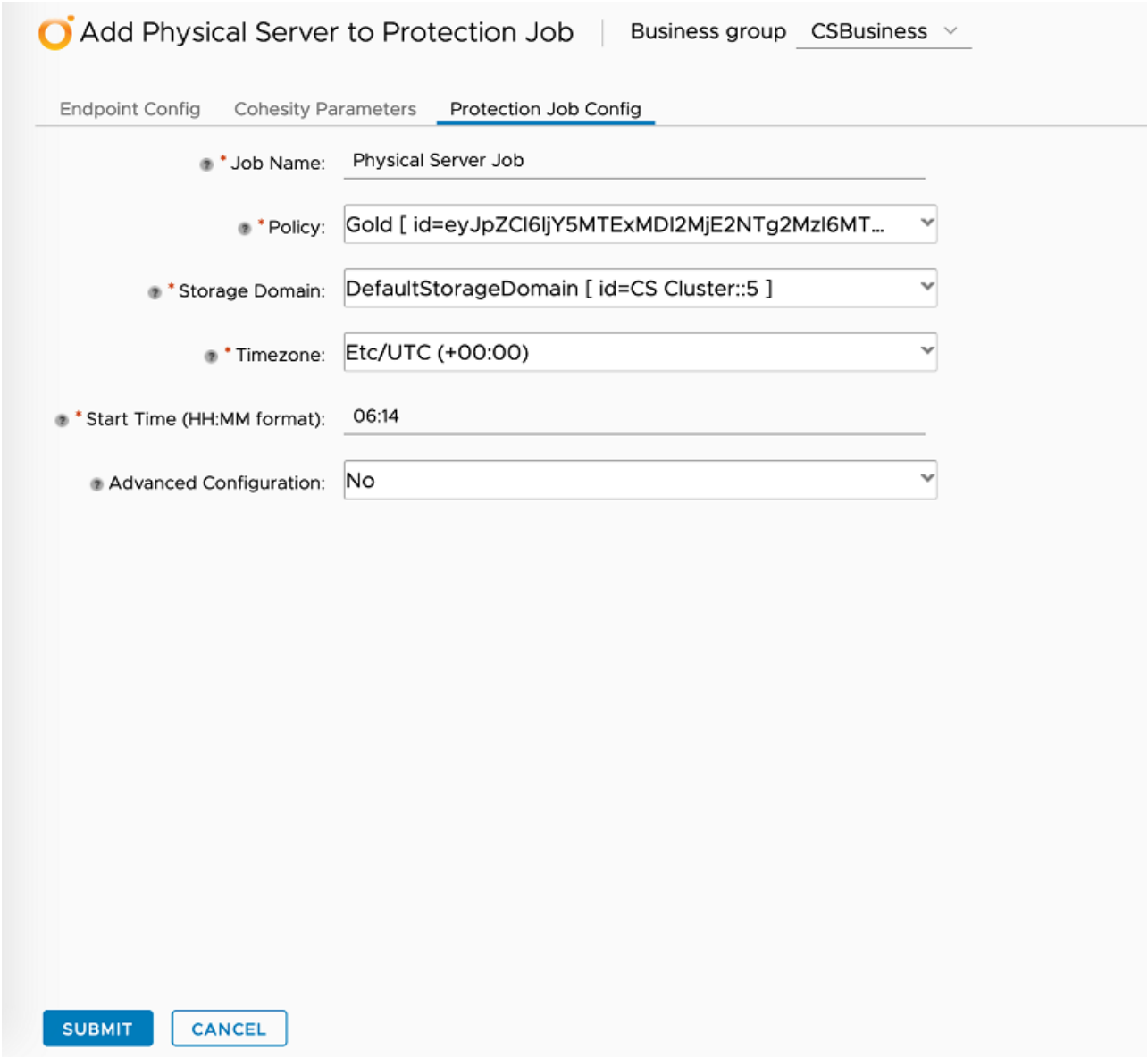
Below is the **Configuration** for ***Block Based*** Protection Type:

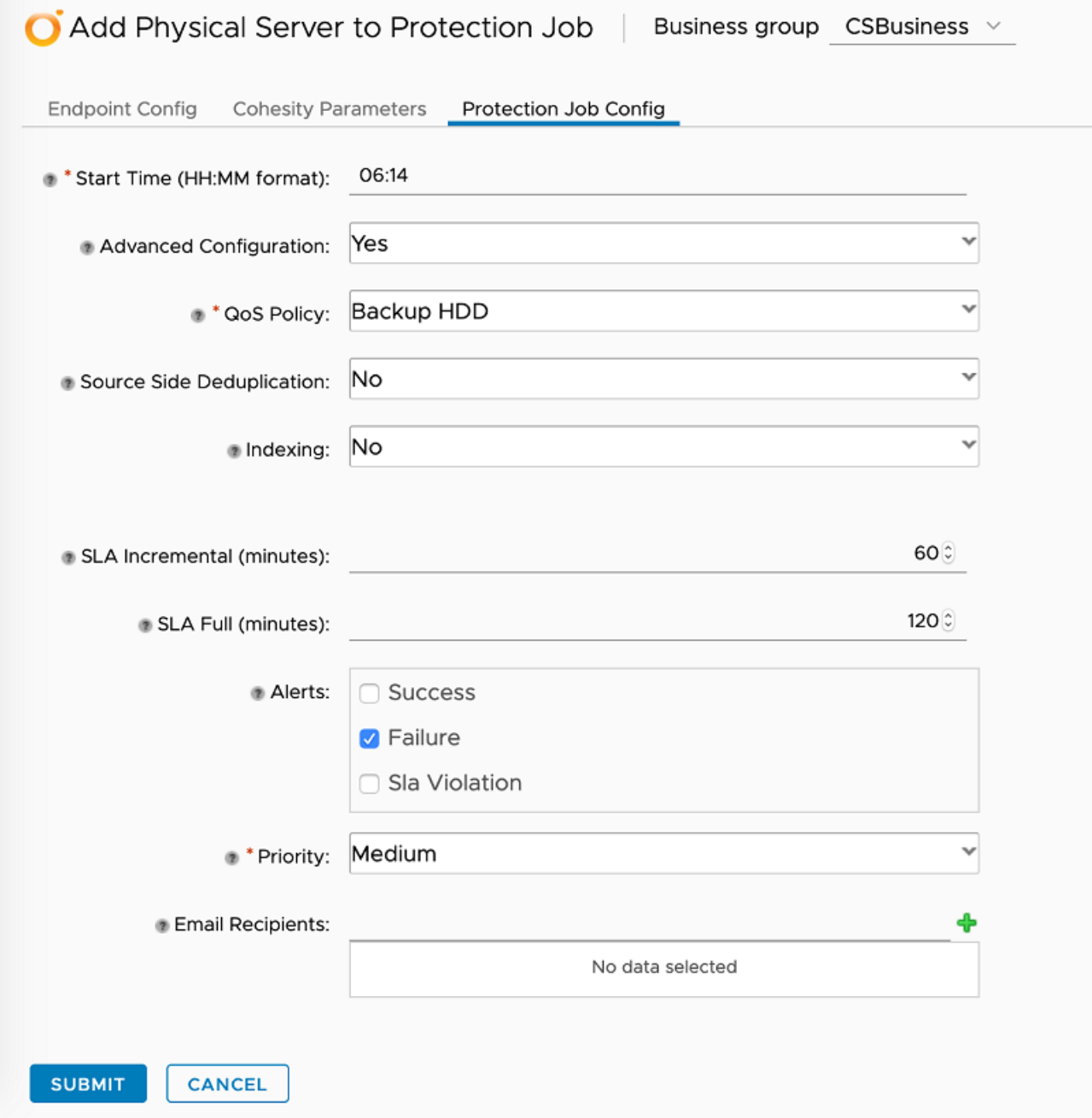


4. Select the corresponding **Physical Server Instance** from the drop down list. **Note**: Only the physical servers that are not protected will be displayed in the drop down.

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 Group, click **Yes**. A new tab **Protection Group 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



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

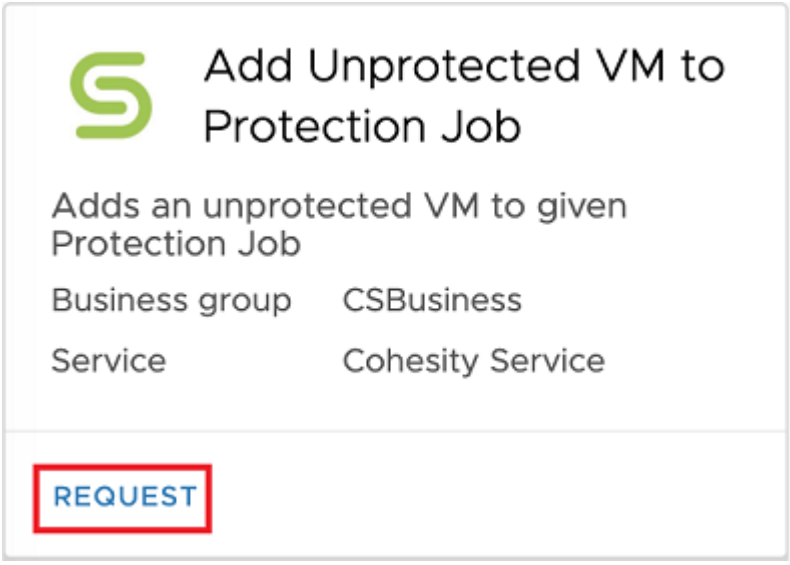
8. Click **Submit**.

Adding an Unprotected VM to Protection Group

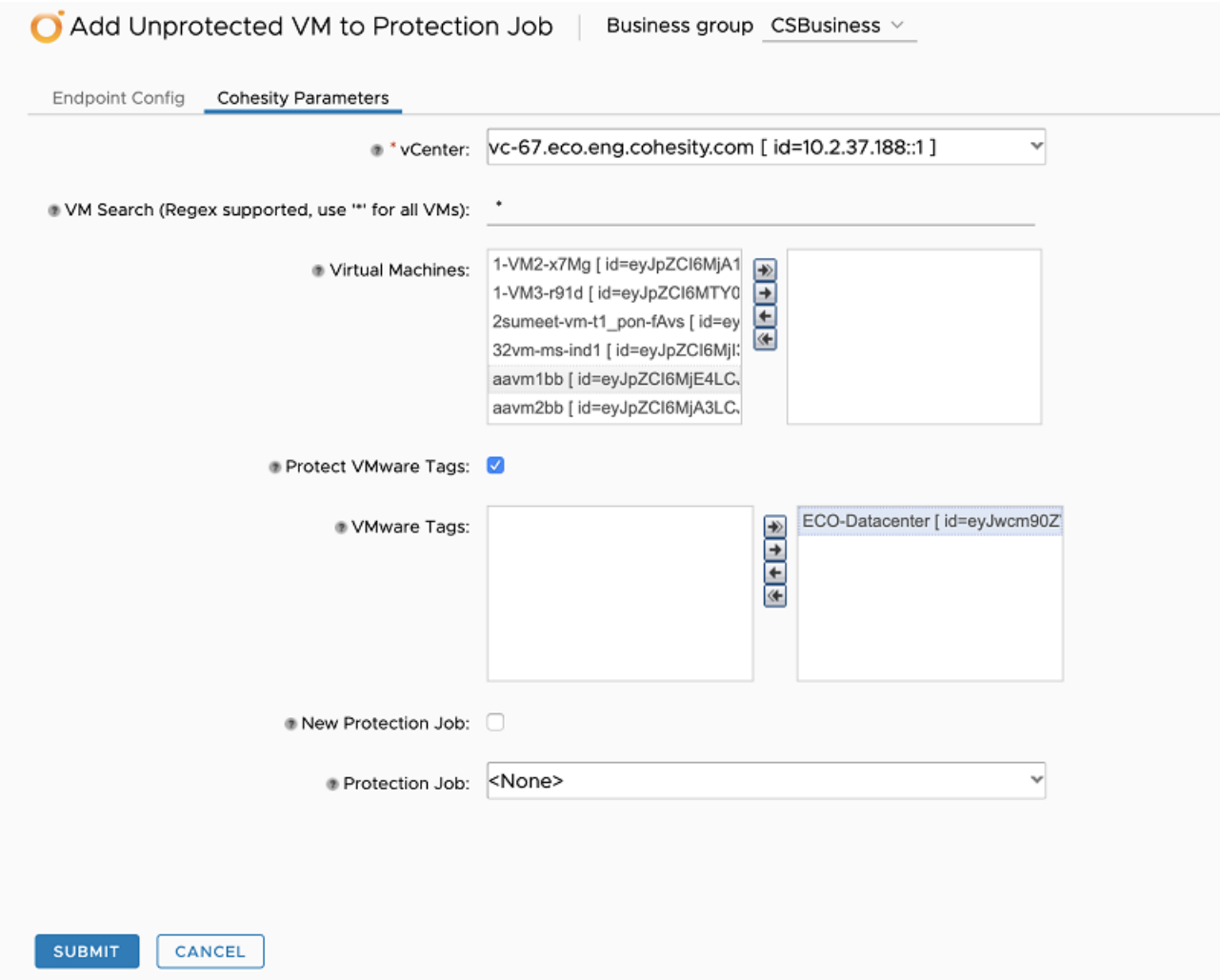
Procedure (XAAS)

To add an unprotected VM to a Protection Group:

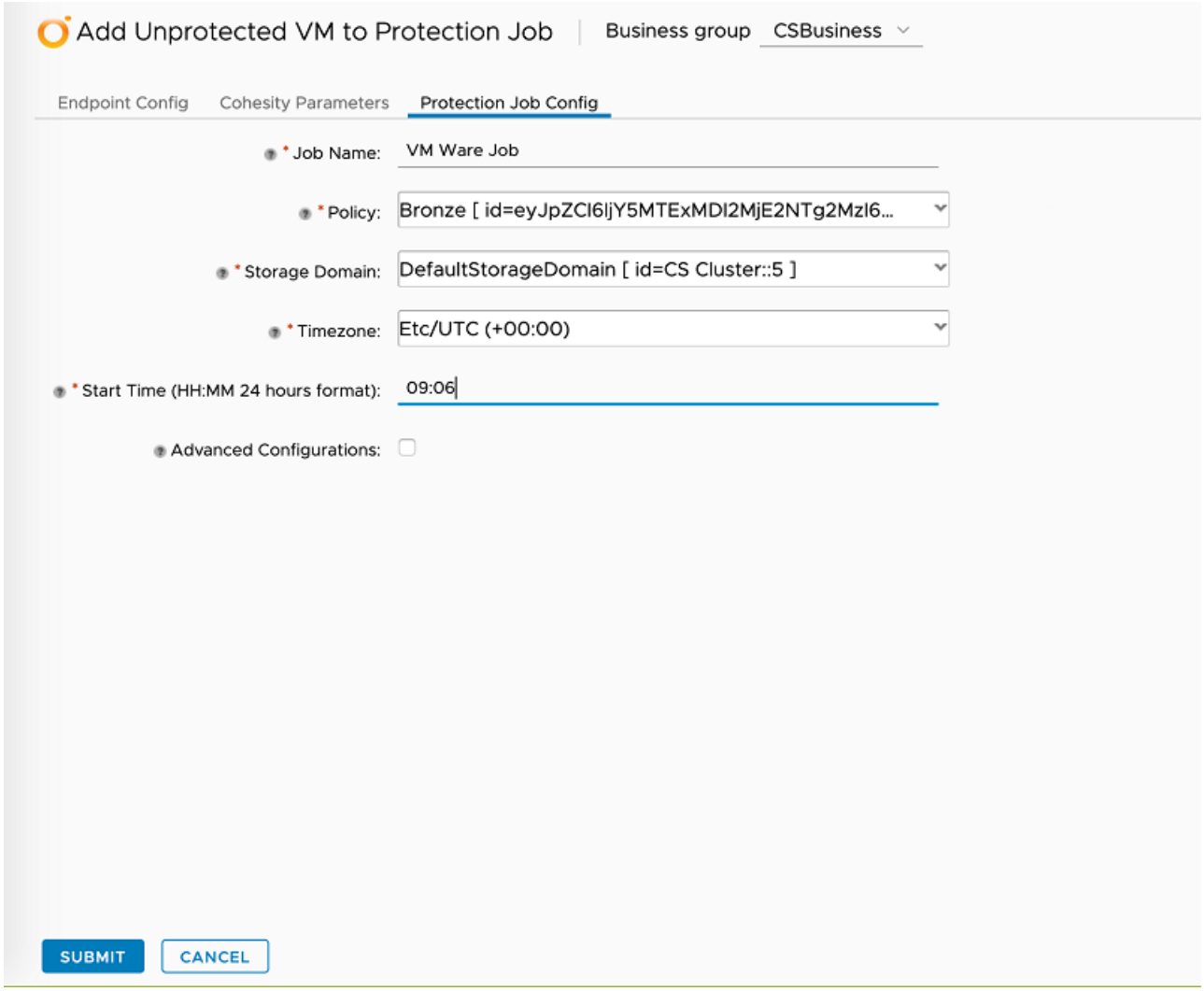
1. In the Catalog Dashboard, click **REQUEST** on **Add Unprotected VM to Protection Group**.

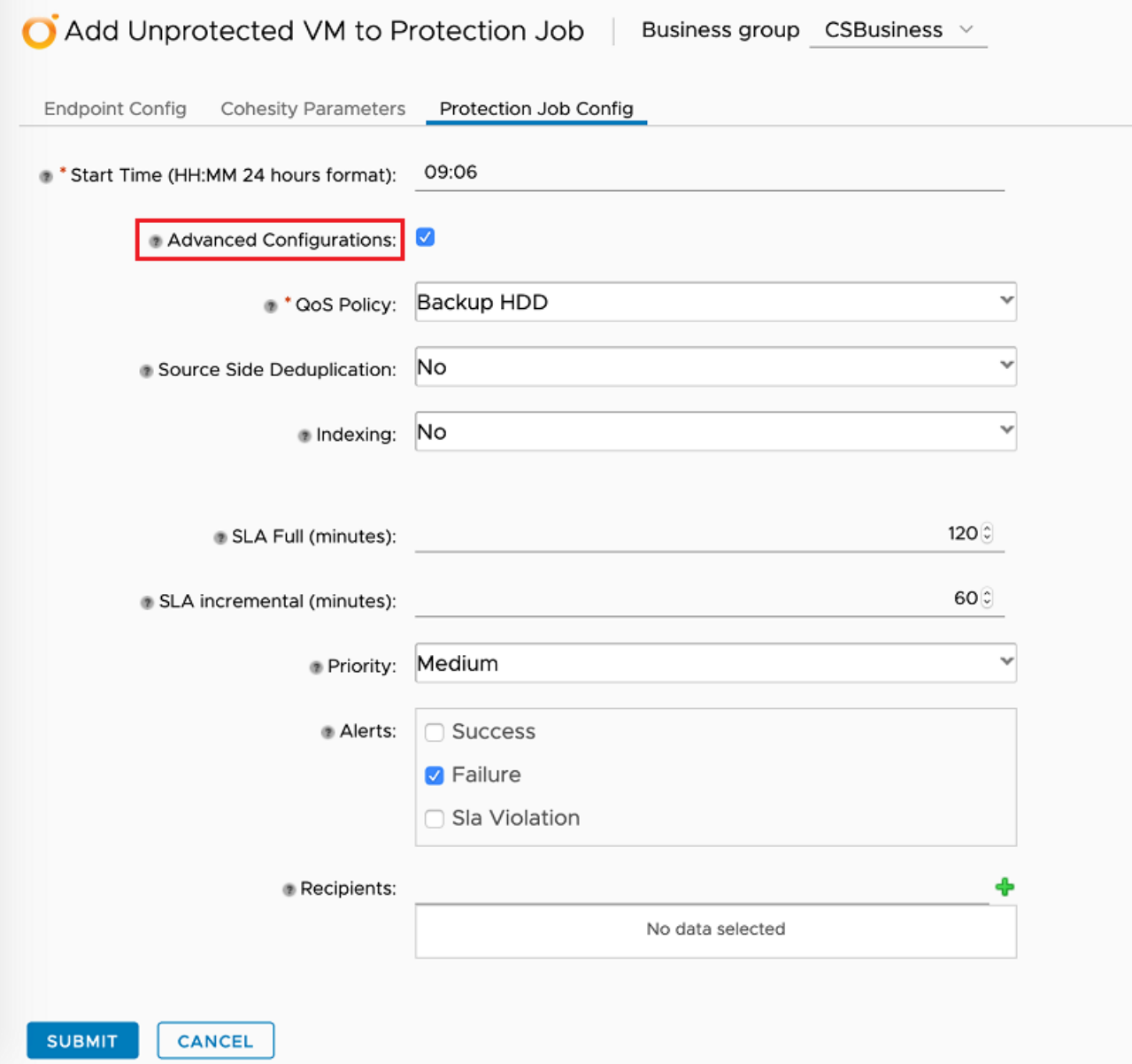


2. From the **Endpoint Config** tab, select the **Cohesity Endpoint** from the drop down list.
3. Click **Cohesity Parameters** tab, and select the **vCenter** from the drop down and select the specific **Virtual Machines** to be protected by moving the VMs from left to right pane. **Note**: In the drop 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 Group > 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 Group 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 Group** by selecting **Yes/No**. If you have selected Yes, then a new tab **Protection Group Config** is displayed.

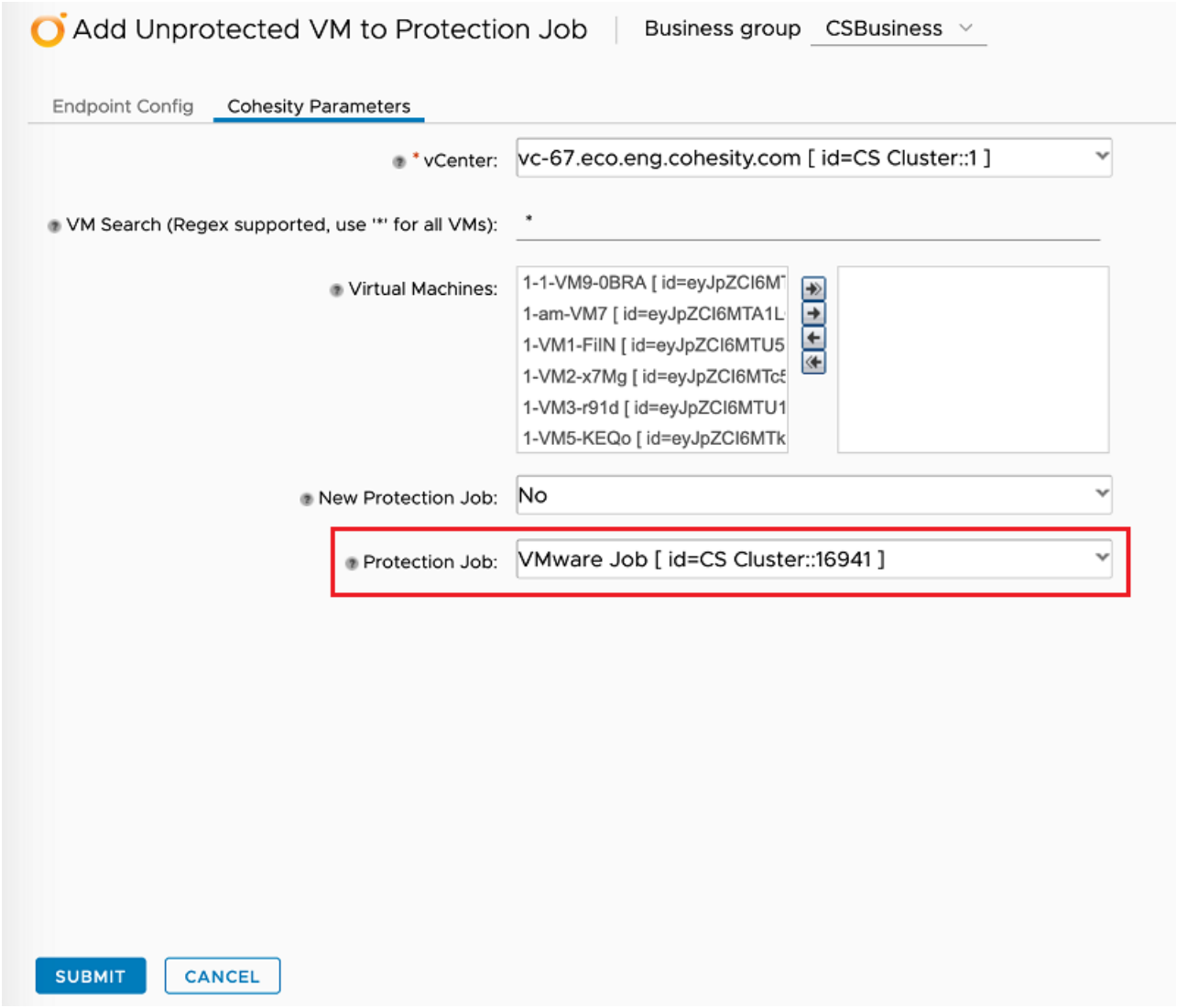


6. Configure all the parameters to create a new job, click **Advanced Configurations** to proceed and complete all the configurations.


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



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



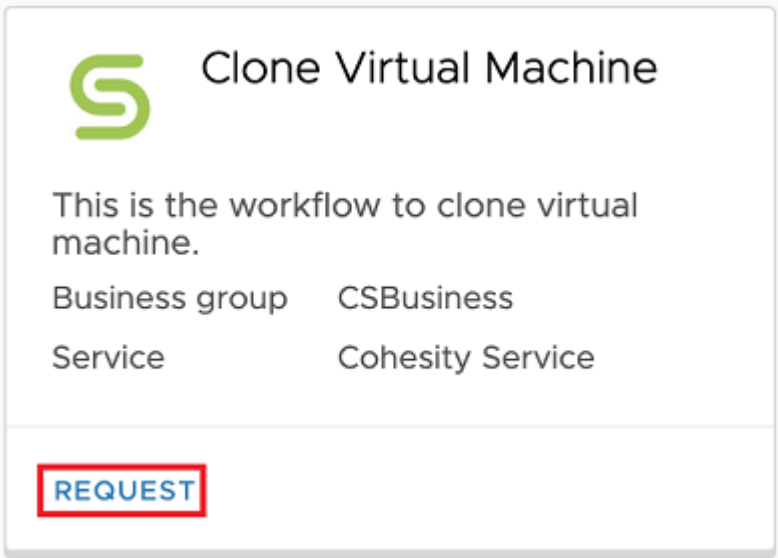
8. Click **Submit**. You can monitor the progress of the request in the **Deployments** tab.

Cloning a Virtual Machine

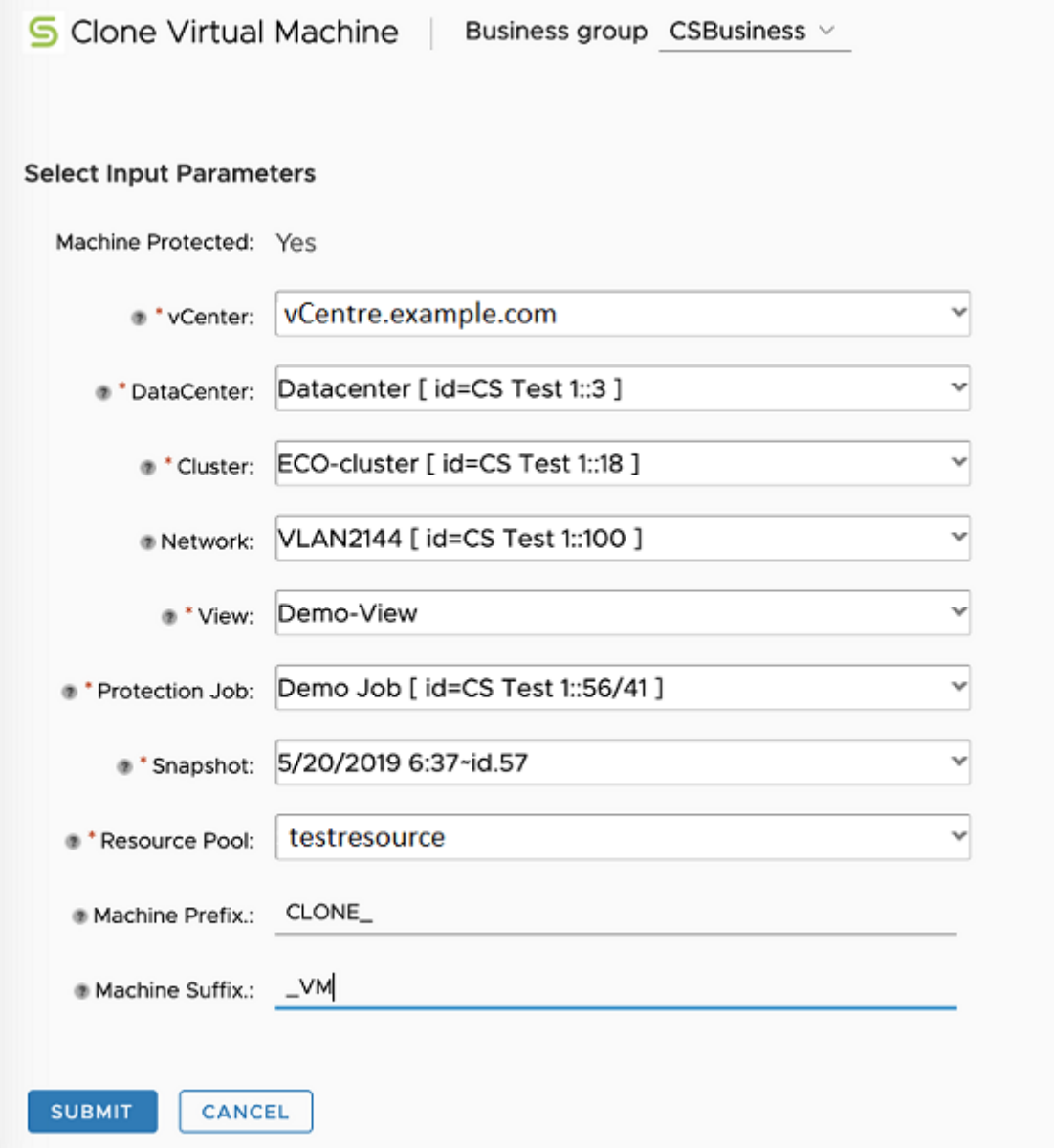
Procedure (XAAS)

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 Group**, **Resource Pool**, **View**, **Snapshot**, **Machine Prefix** and **Machine Suffix** from the corresponding drop down list.



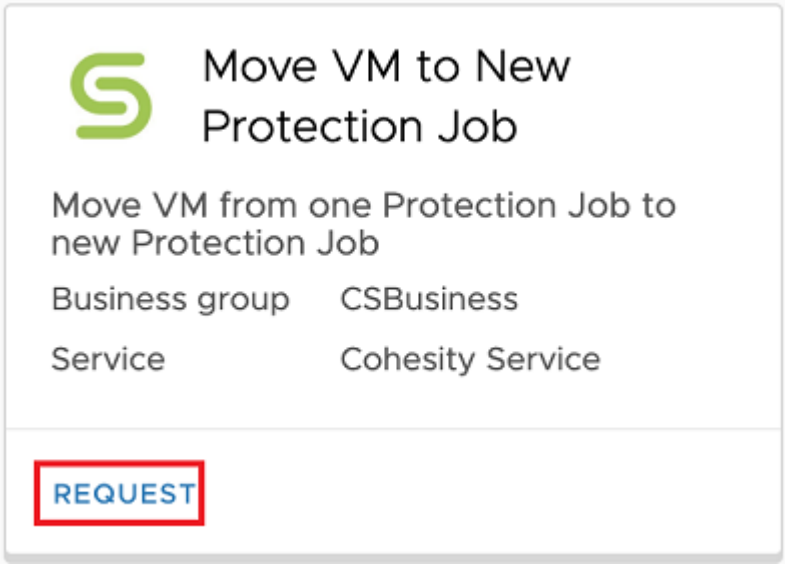
5. Click **Submit**.

Moving a VM to a New Protection Group

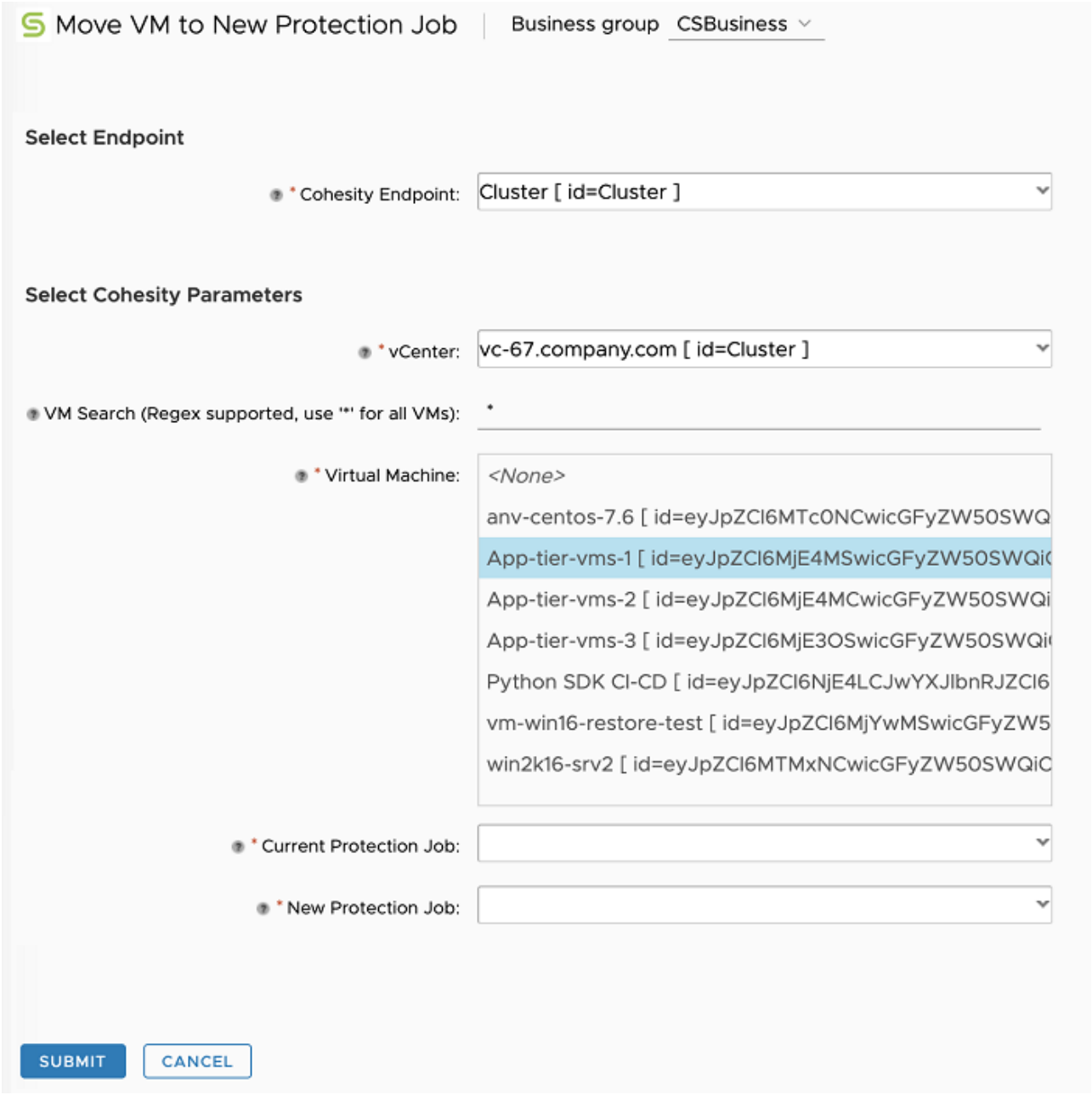
Procedure (XAAS)

You can move a VM to a new Protection Group as follows.

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



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 Group**, and **New Protection Group** it must be assigned to. **Note**: In the drop down list for Virtual Machines, only the protected VMs are displayed.



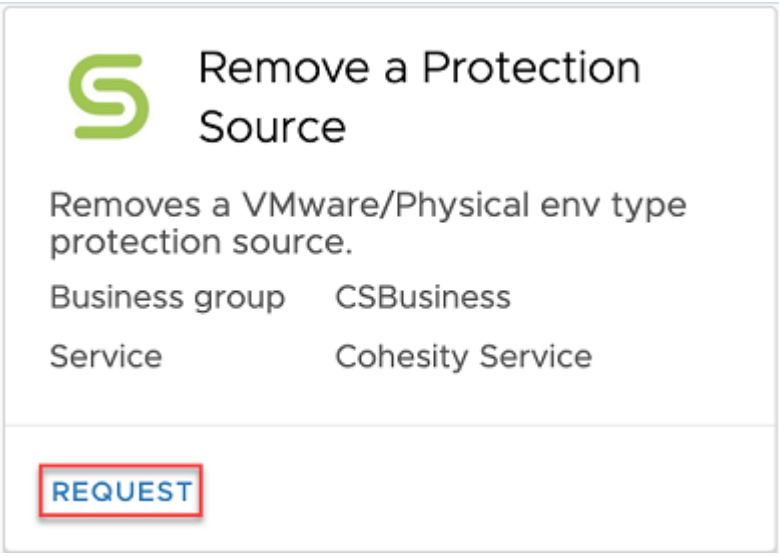
4. Click **Submit**.

Removing a Protection Source

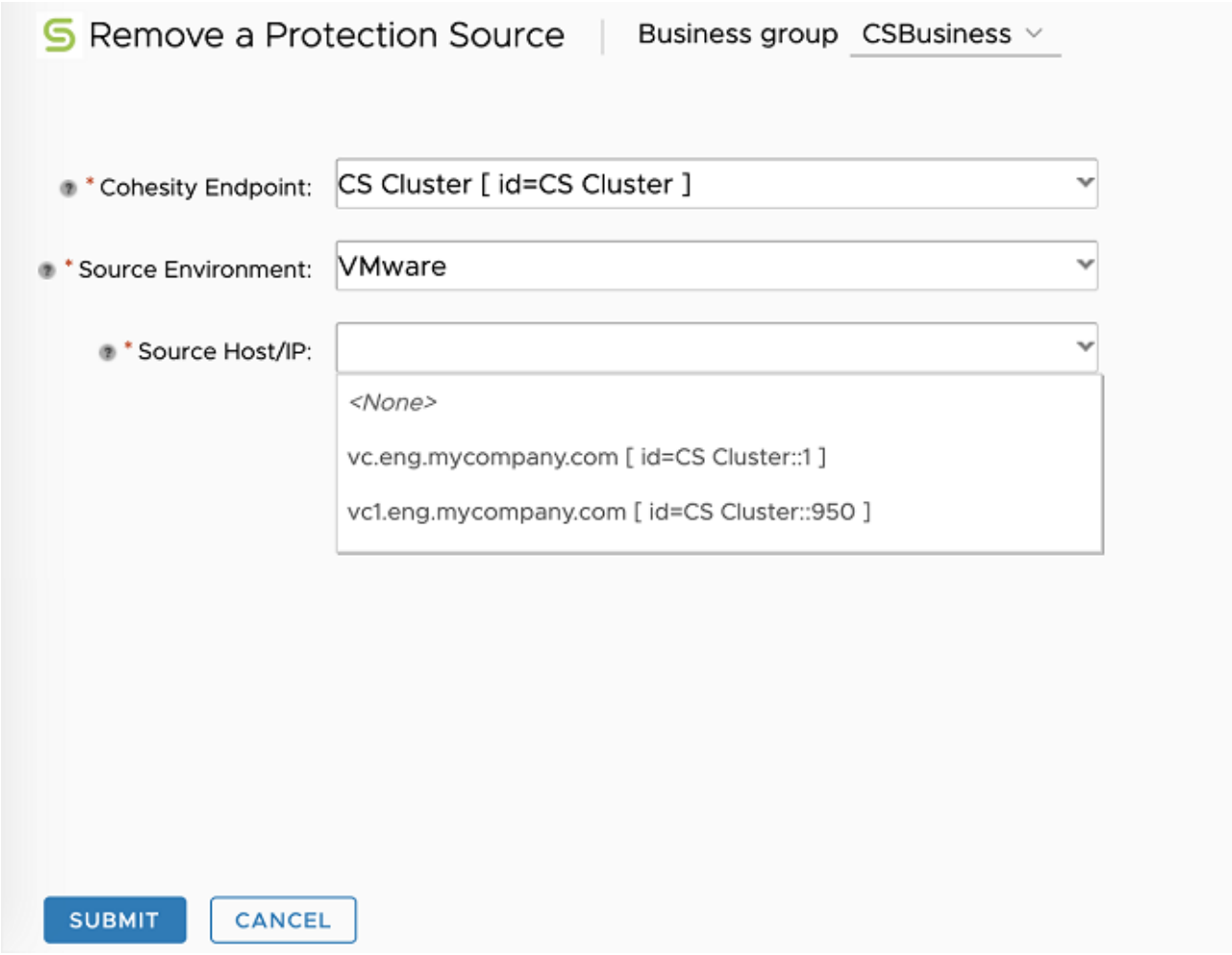
To remove a VMware or a physical server as a protection source:

Procedure (XAAS)

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



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



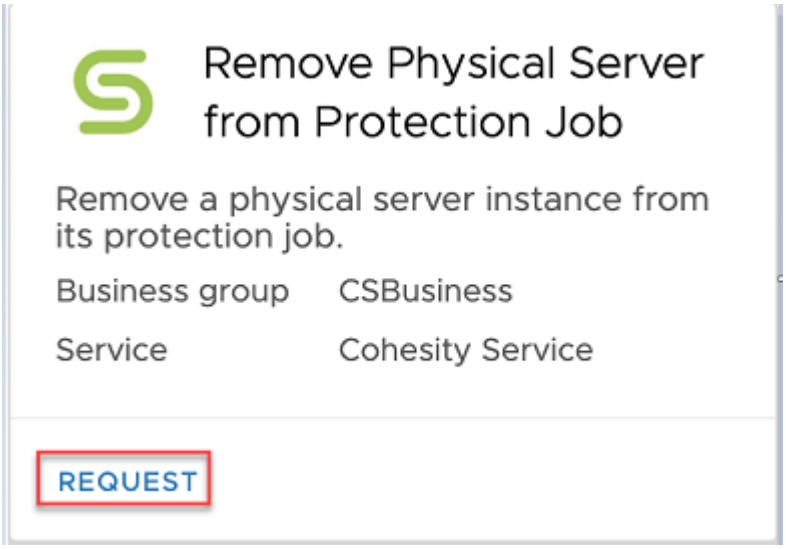
3. Click **Submit**.
   Note: If there is already an active Protection Group that is protecting a virtual machine of vCentre, you cannot remove that virtual machine. If you wish to remove the protection source, then either the Protection Group must be made inactive or the source must be removed from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

Removing Physical Server from Protection Group

Procedure (XAAS)

To remove a physical server instance from its Protection Group:

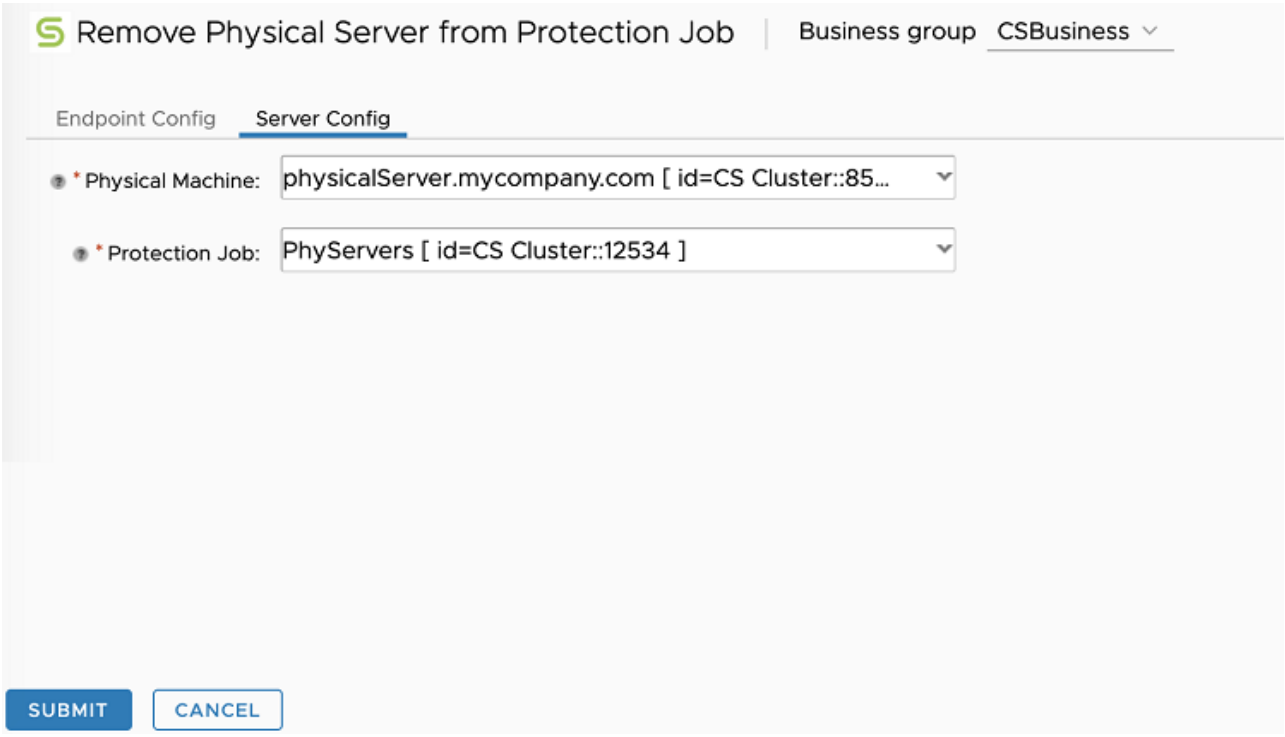
1. In the Catalog Dashboard, click **REQUEST** on **Remove Physical Server from Protection Group**.



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

3. Under **Server Config** tab, select the **Physical Machine** and **Protection Group** 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 Group which has only 1 physical machine associated, then you cannot remove that physical machine from the job. A Protection Group will always be associated or will always protect at least one Physical machine.



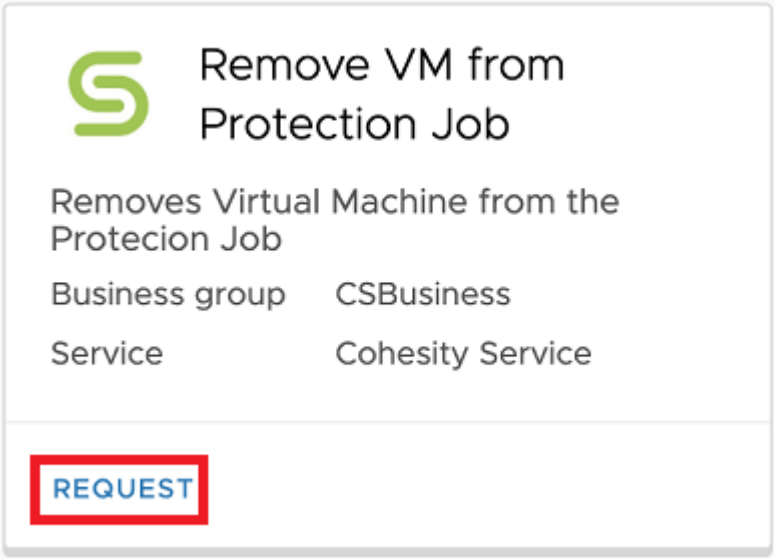
4. Click **Submit**.

Removing a VM from a Protection Group

Procedure (XAAS)

To remove a VM from a Protection Group:

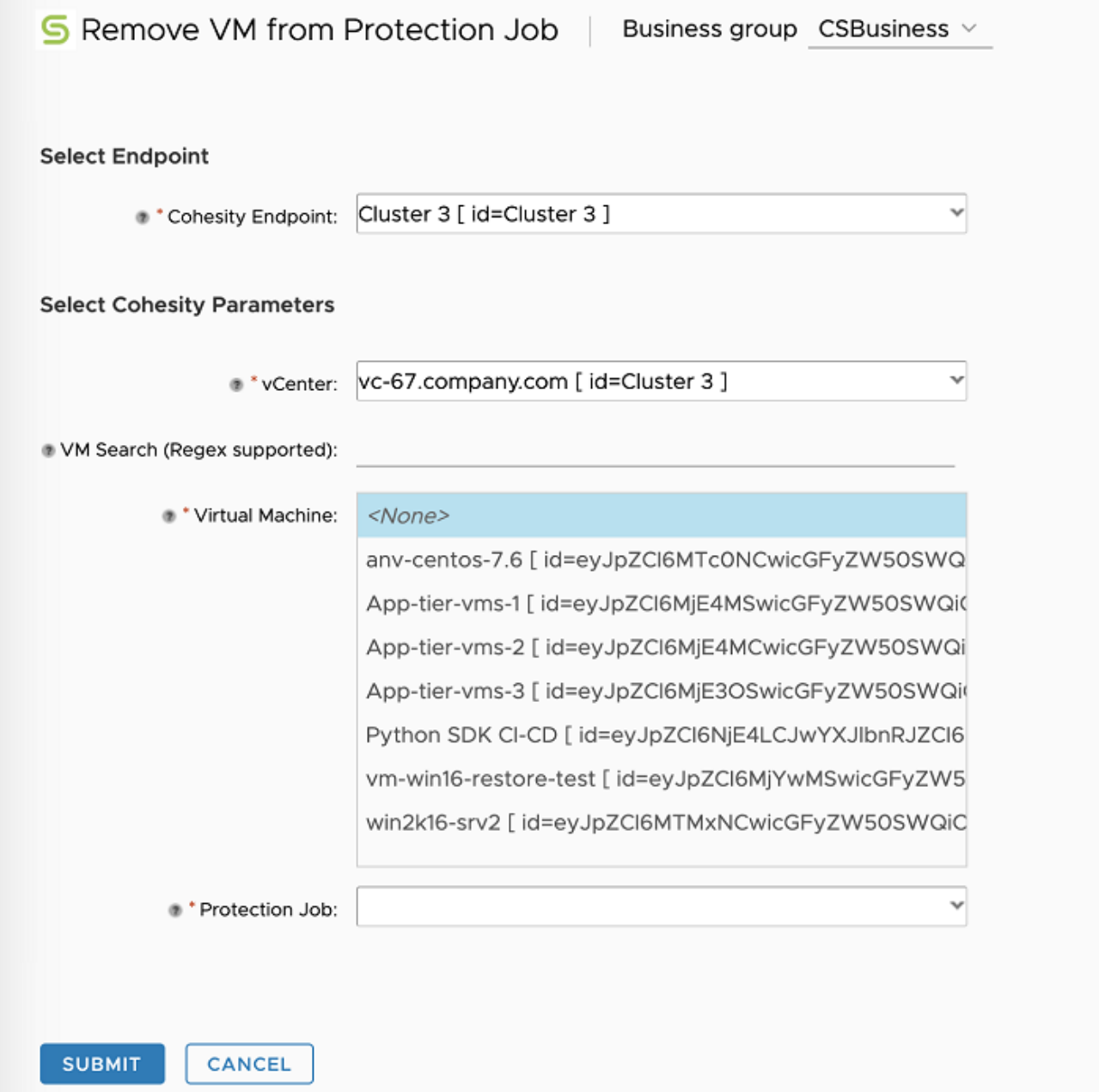
1. In the Catalog Dashboard, click **REQUEST** on **Remove VM from Protection Group**.



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 Group**. **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 Group**.



Note

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

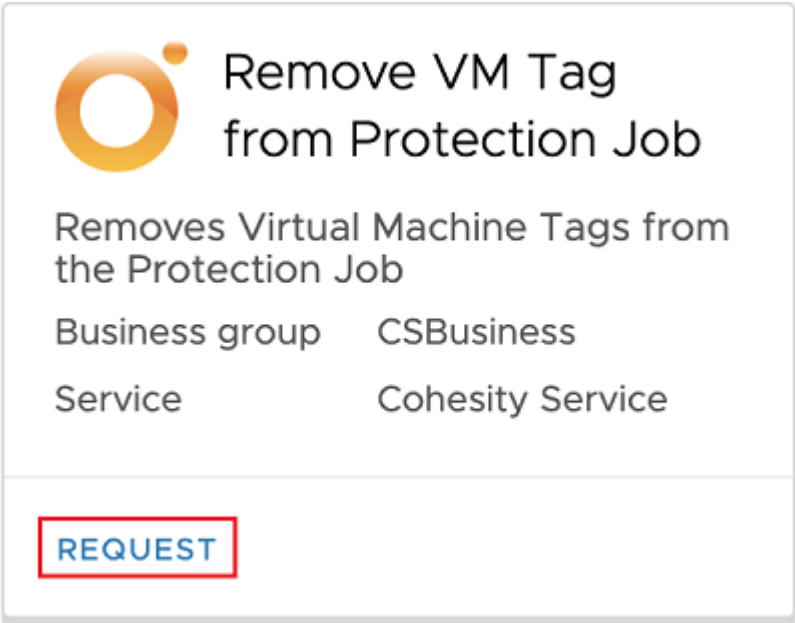
4. Click **Submit**.

Removing VM Tag from Protection Group

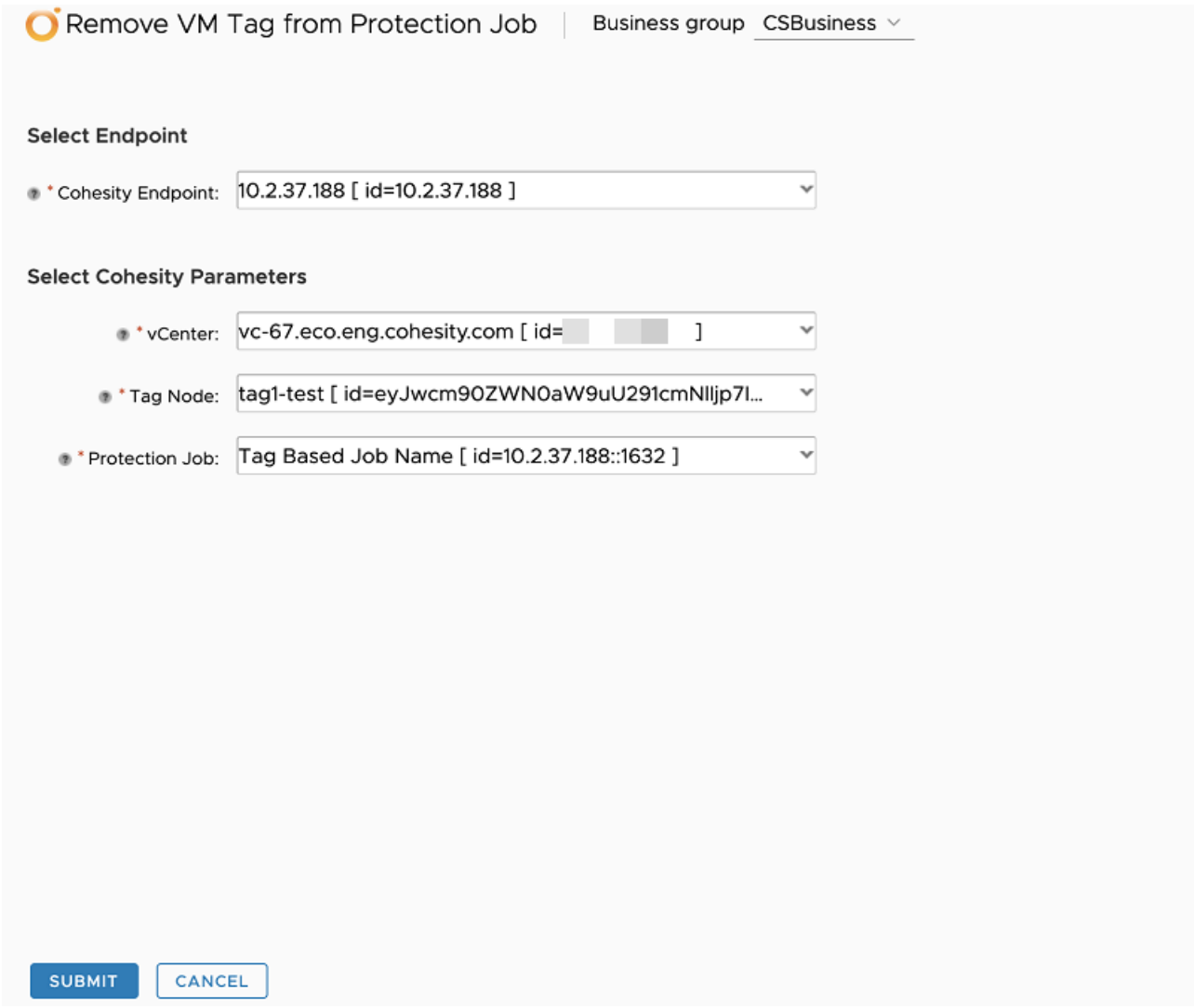
Procedure (XAAS)

To unprotect the VMware tags:

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



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 Group that is protecting the tags will be automatically displayed. **Note**: Only the tags assigned to VMs will be displayed here.



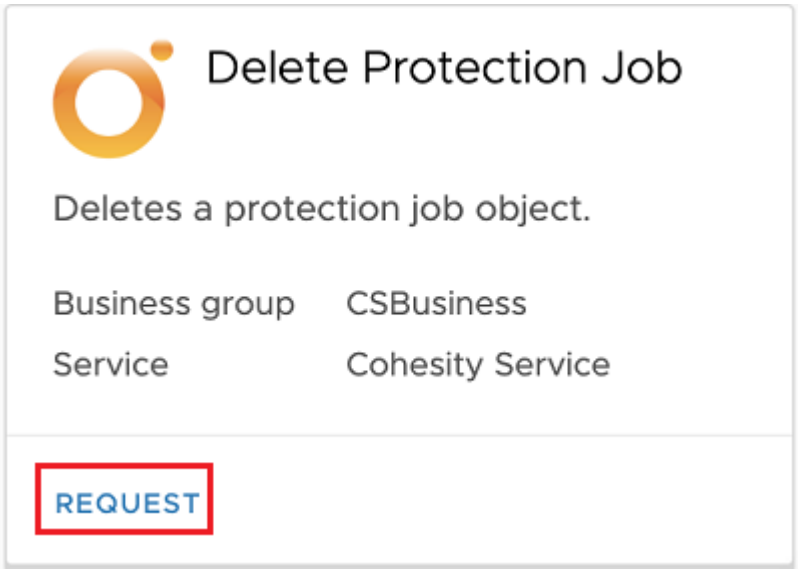
5. Click **Submit**.

Deleting a Protection Group

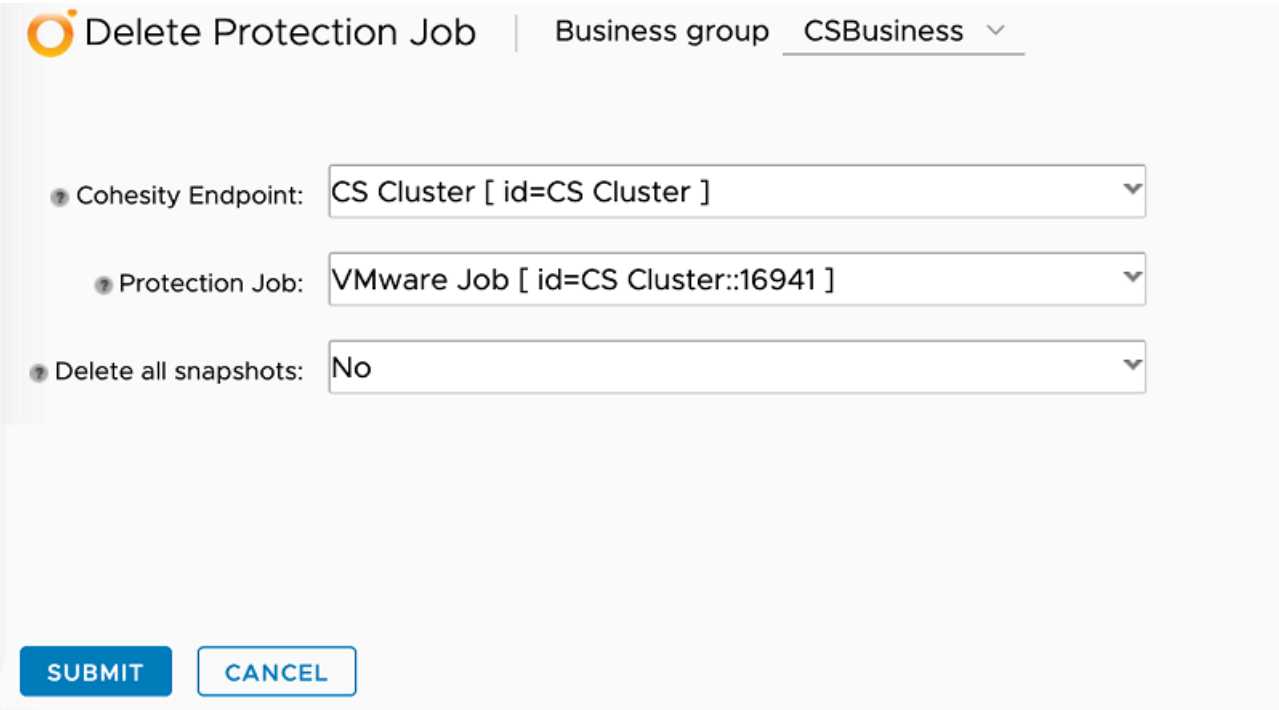
Procedure (XAAS)

To delete a Protection Group object:

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



2. Select the **Cohesity Endpoint** and the **Protection Group** 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 Group while the back up taken for that system will be retained).



4. Click **Submit**.

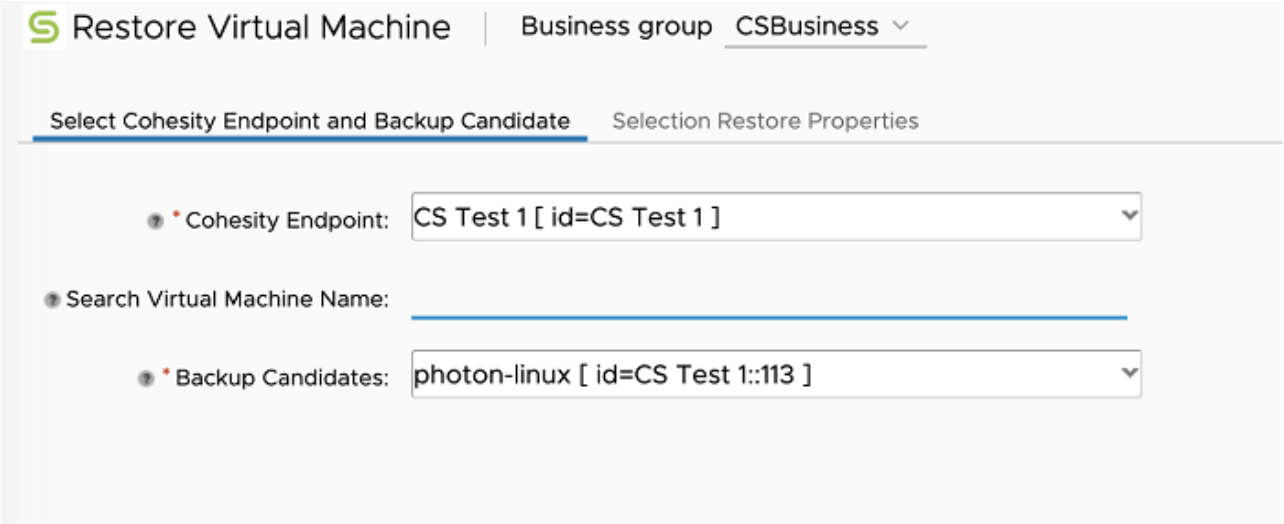
Restoring a Virtual Machine

Procedure (XAAS)

To restore a VM:

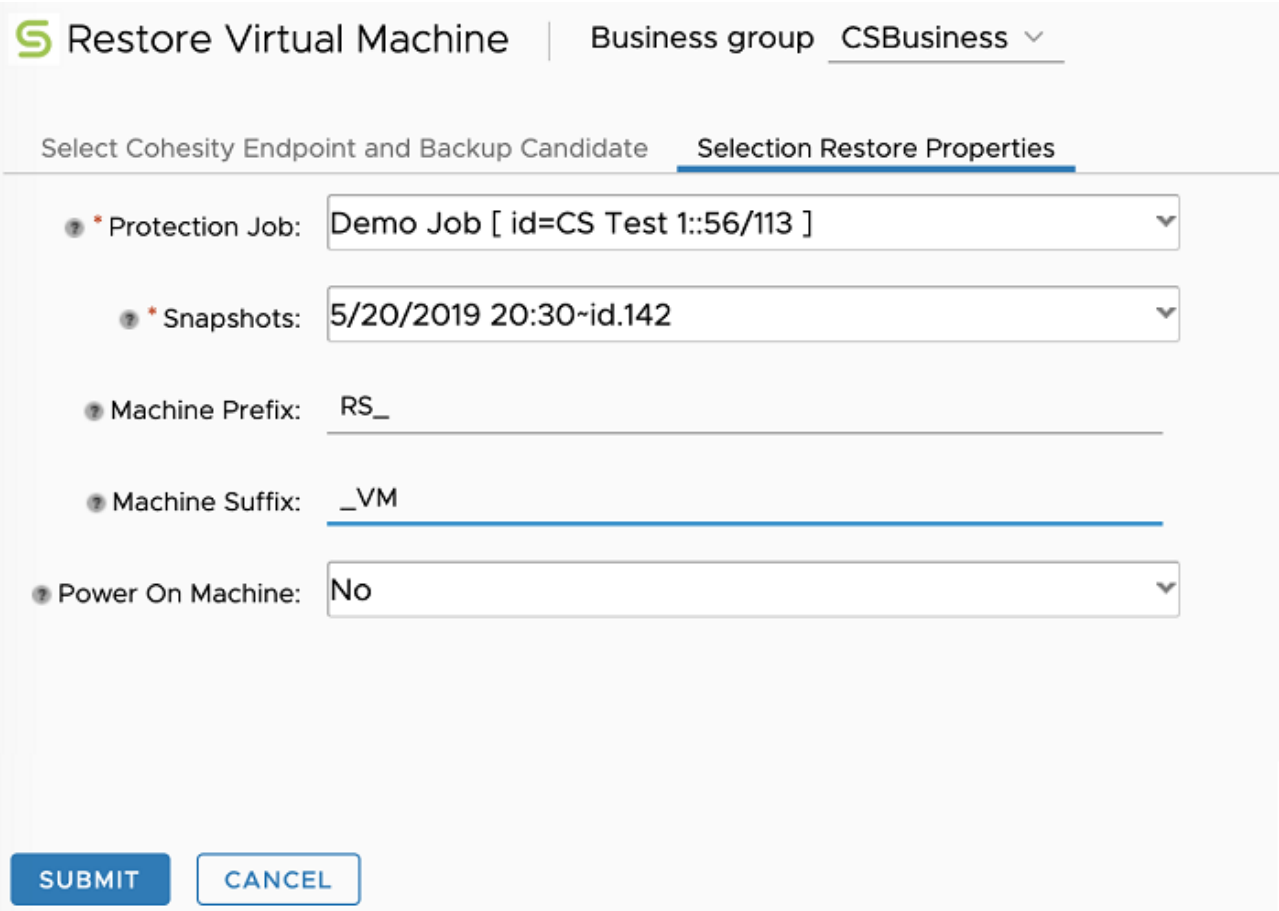
1. In the Catalog Dashboard, click **REQUEST** on **Restore Virtual Machine**.

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.



3. Click **Selection Restore Properties** tab and enter the Protection Group you want to perform the restore from in the **Protection Group** field. Note: The list populated in the drop down of **Protection Group** may contain multiple values if the backup candidate is protected by multiple jobs.
4. Select the **Snapshot** from which you want to execute the restore.
5. Optionally, you can provide the **Machine Prefix** and **Machine Suffix**.

6. By default, the VM is powered OFF after restore. Select as required and click **Submit**.

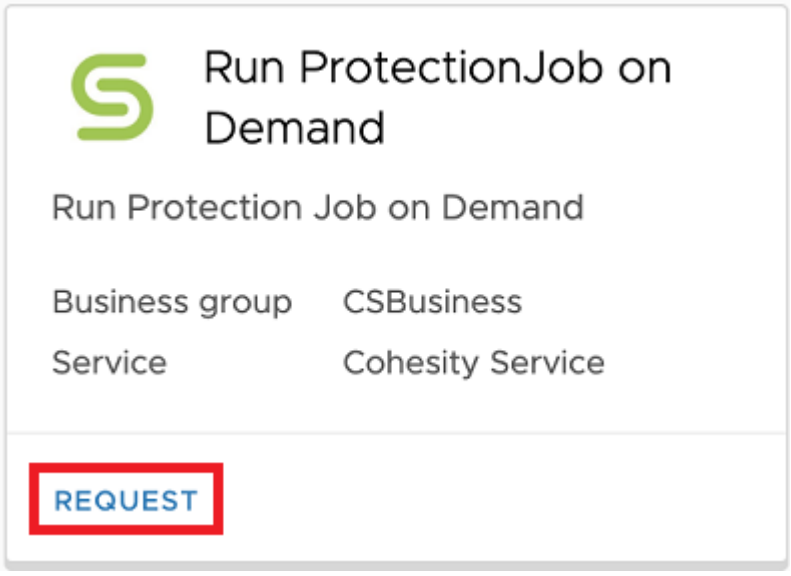


Executing a Protection Group on Demand

Procedure (XAAS)

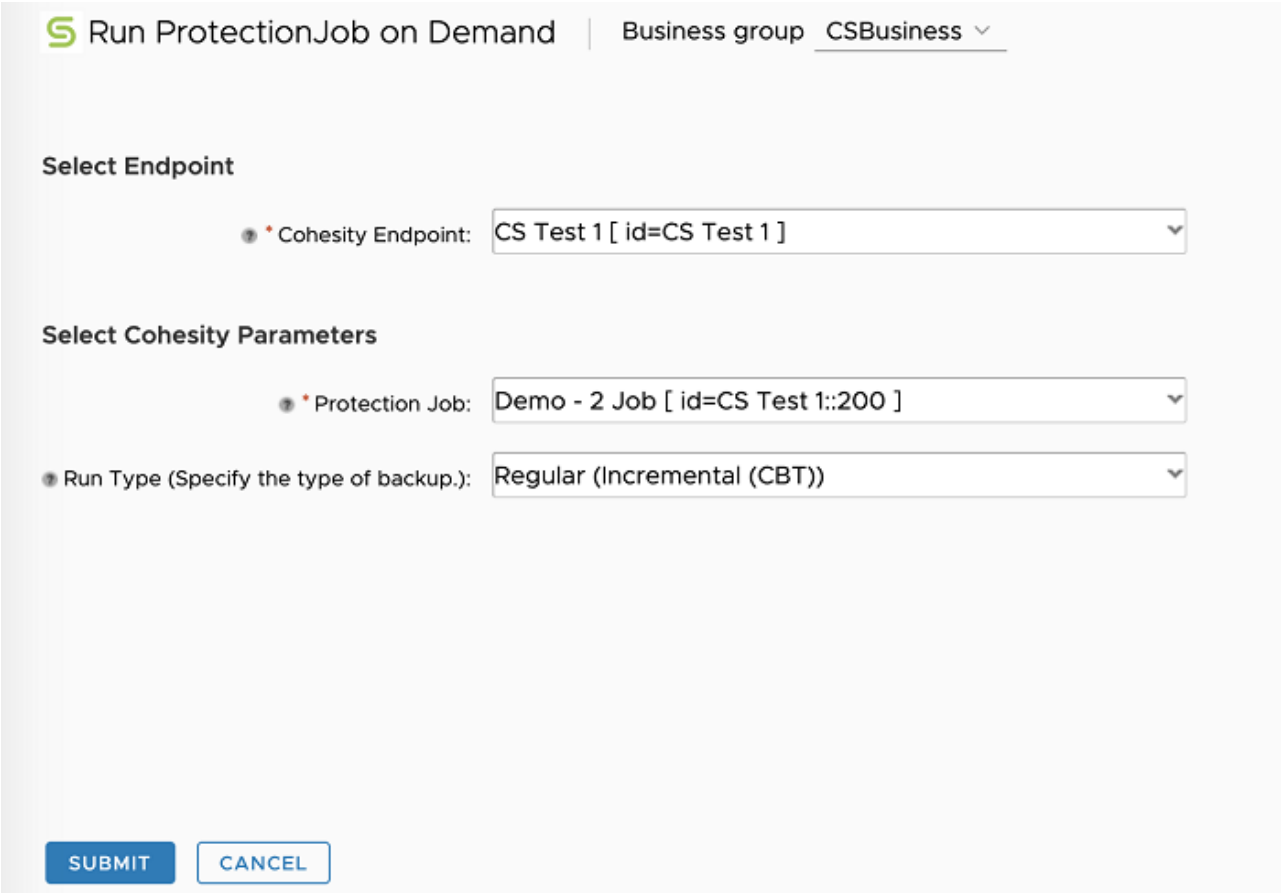
To execute a Protection Group:

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



2. Select the **Cohesity Endpoint** from the drop down list.
3. In the **Protection Group** field, enter the Protection Group you want to execute.

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



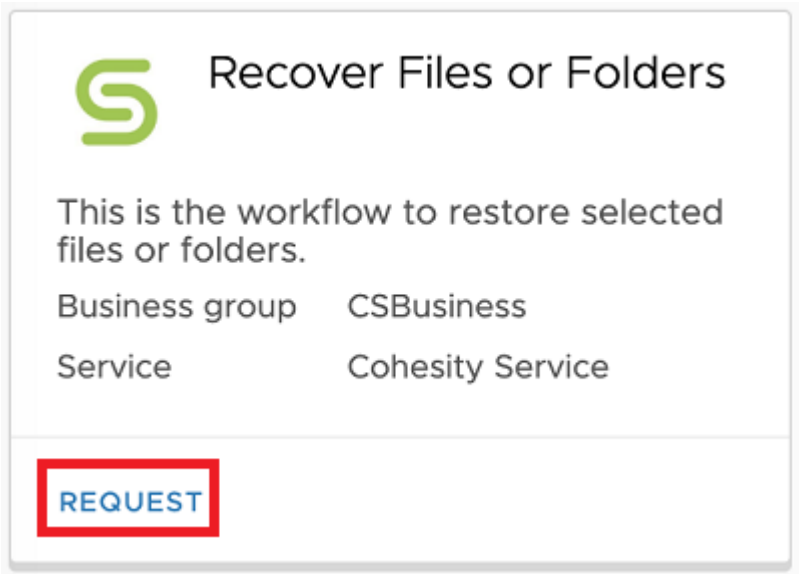
5. Click **Submit**.

Recovering Files or Folders

Procedure (XAAS)

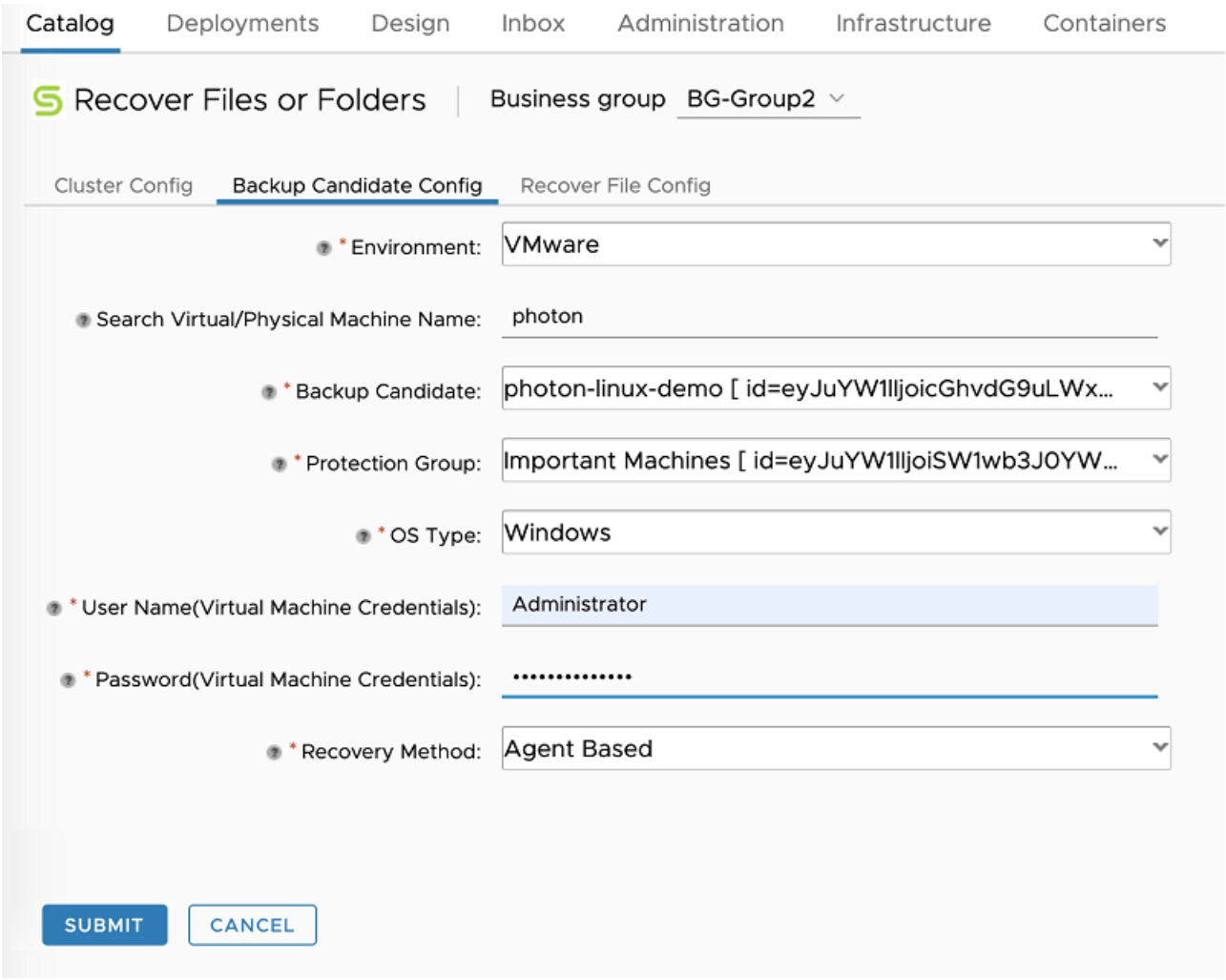
To recover a file or folder:

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.



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 Group. 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.

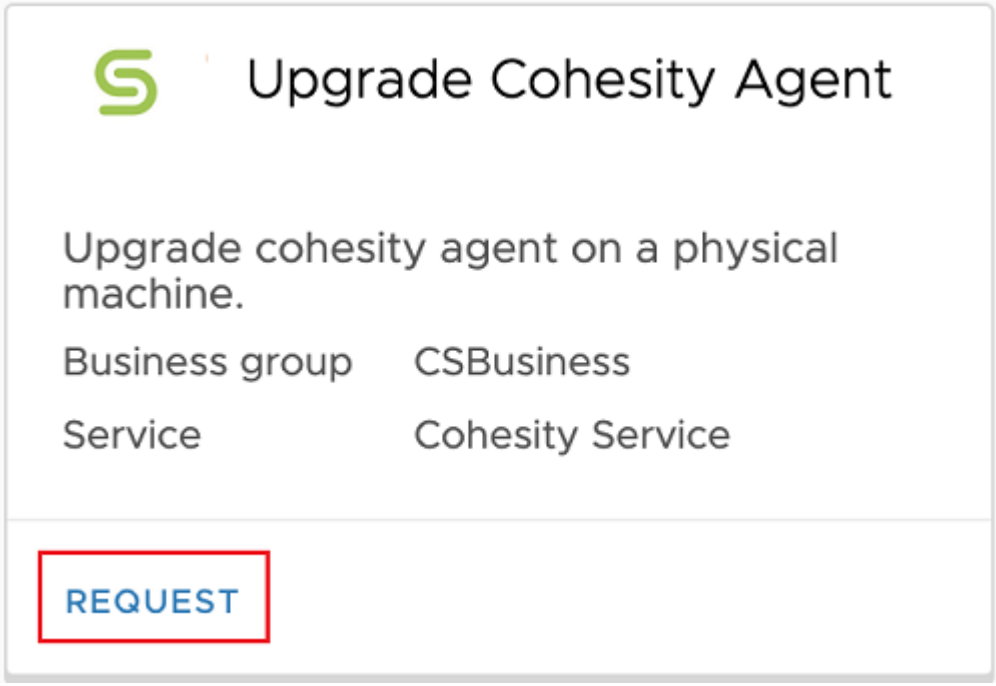
7. Select **Yes** or **No** for **Continue on Error** parameter. If **Yes** is selected, recovery is continued even when there is any error, else recovery stops when there is an error.
8. Select **Yes** or **No** for **Preserve Attributes** parameter.
9. Select **Yes** or **No** for **Send Email Notification**. 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:

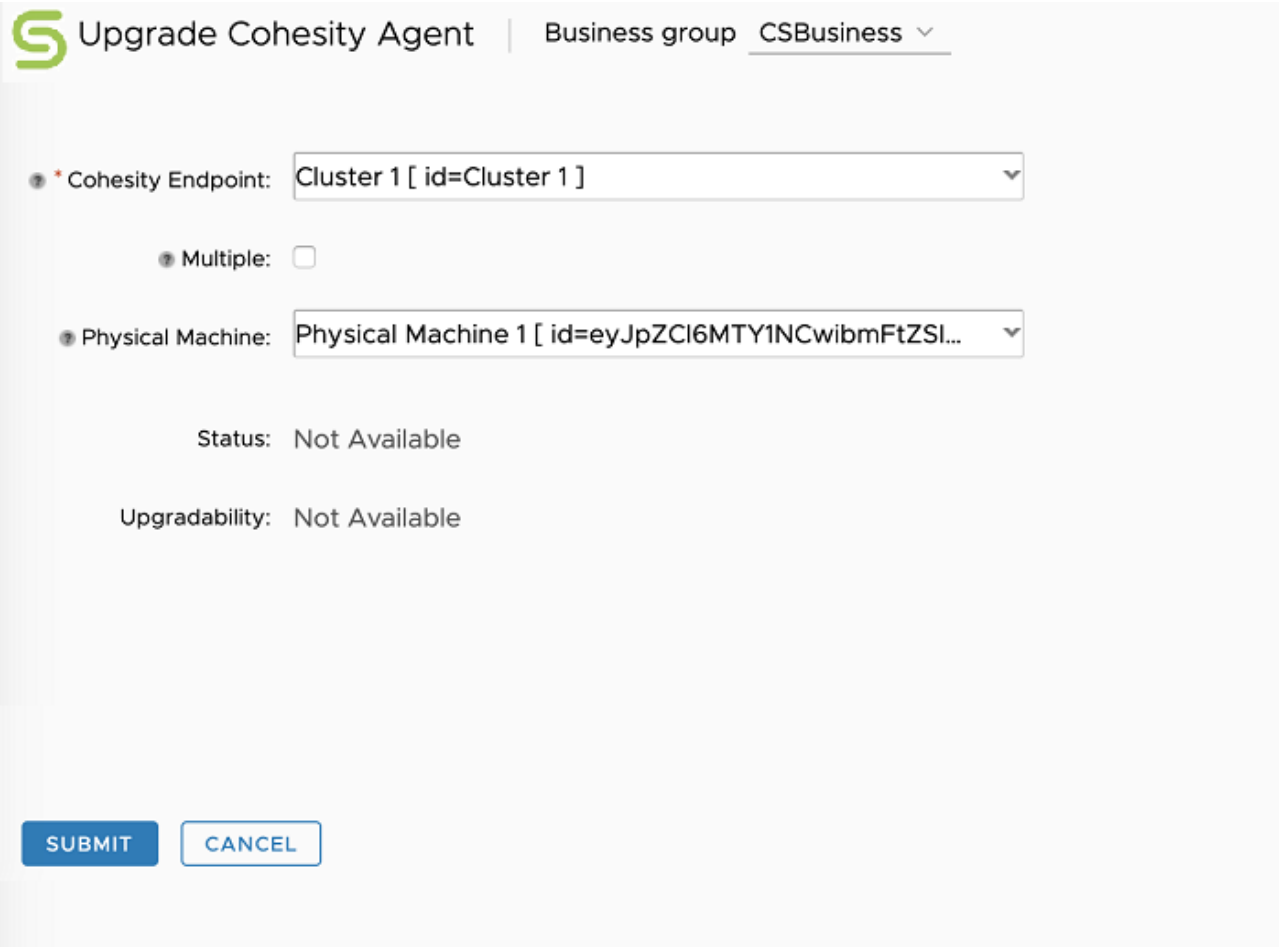
1. In the Catalog Dashboard, click **REQUEST** on **Upgrade Cohesity Agent**.



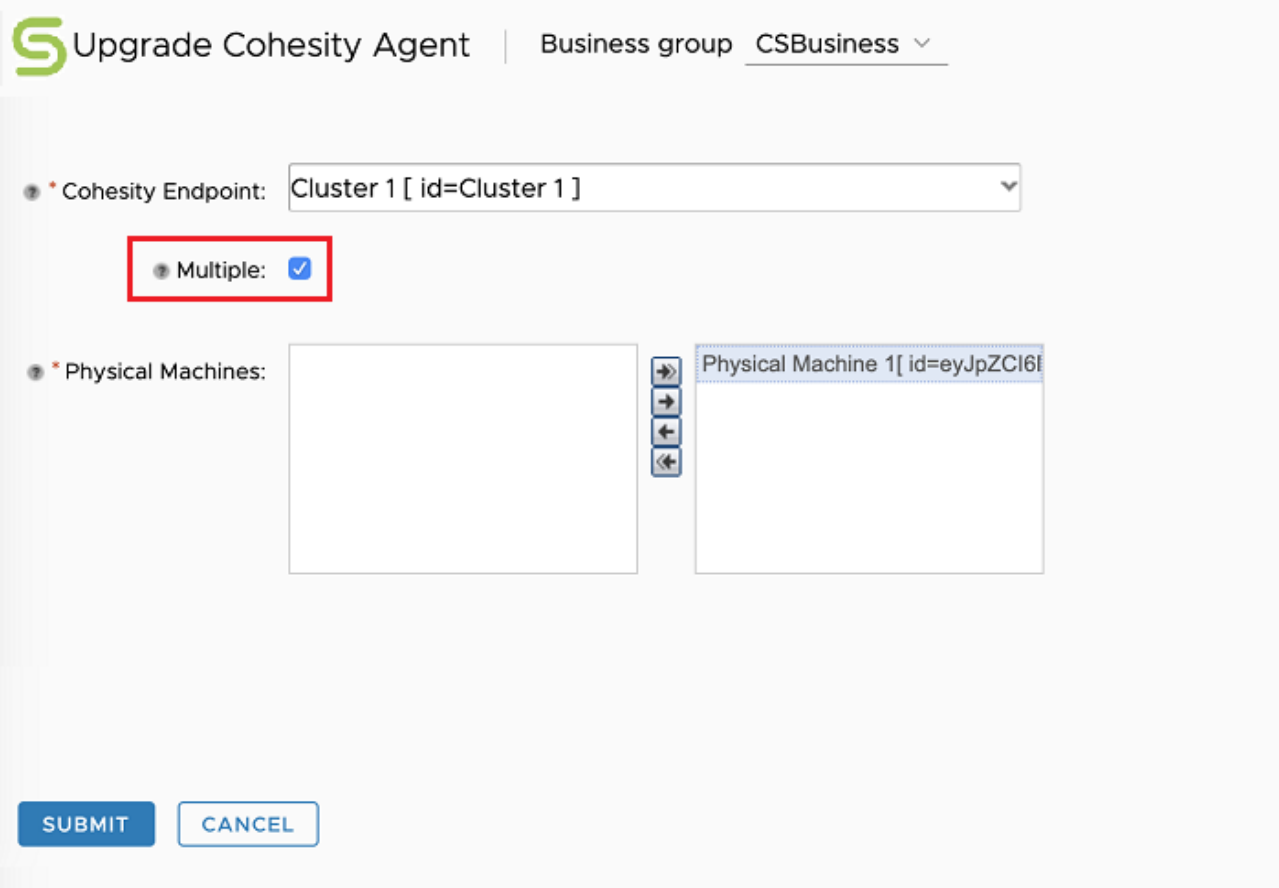
2. Select the **Cohesity Endpoint** from the drop down list.
3. Select the **Physical Machine**.

   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.



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.



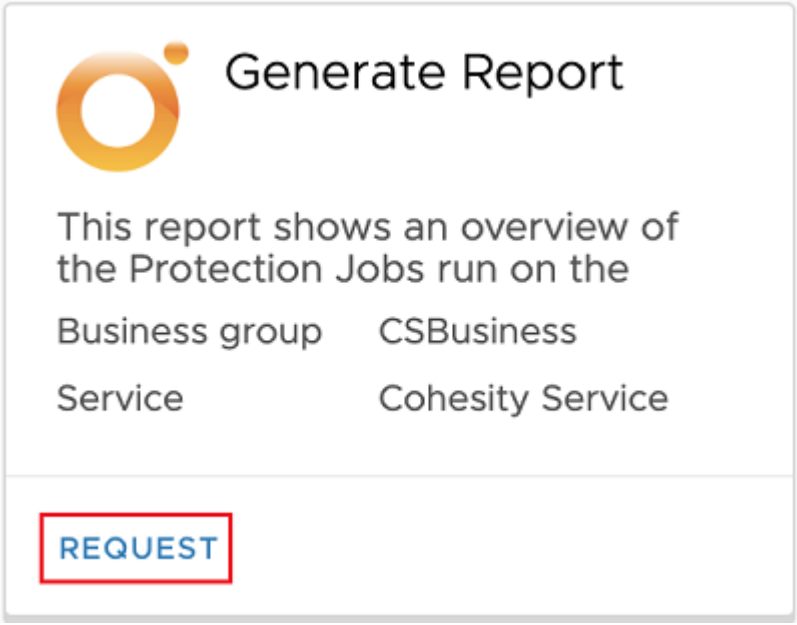
5. Click **Submit**. **Note**: Status of the agent upgrade request cannot be monitored through the workflow if multiple physical sources are selected.

Generating Reports

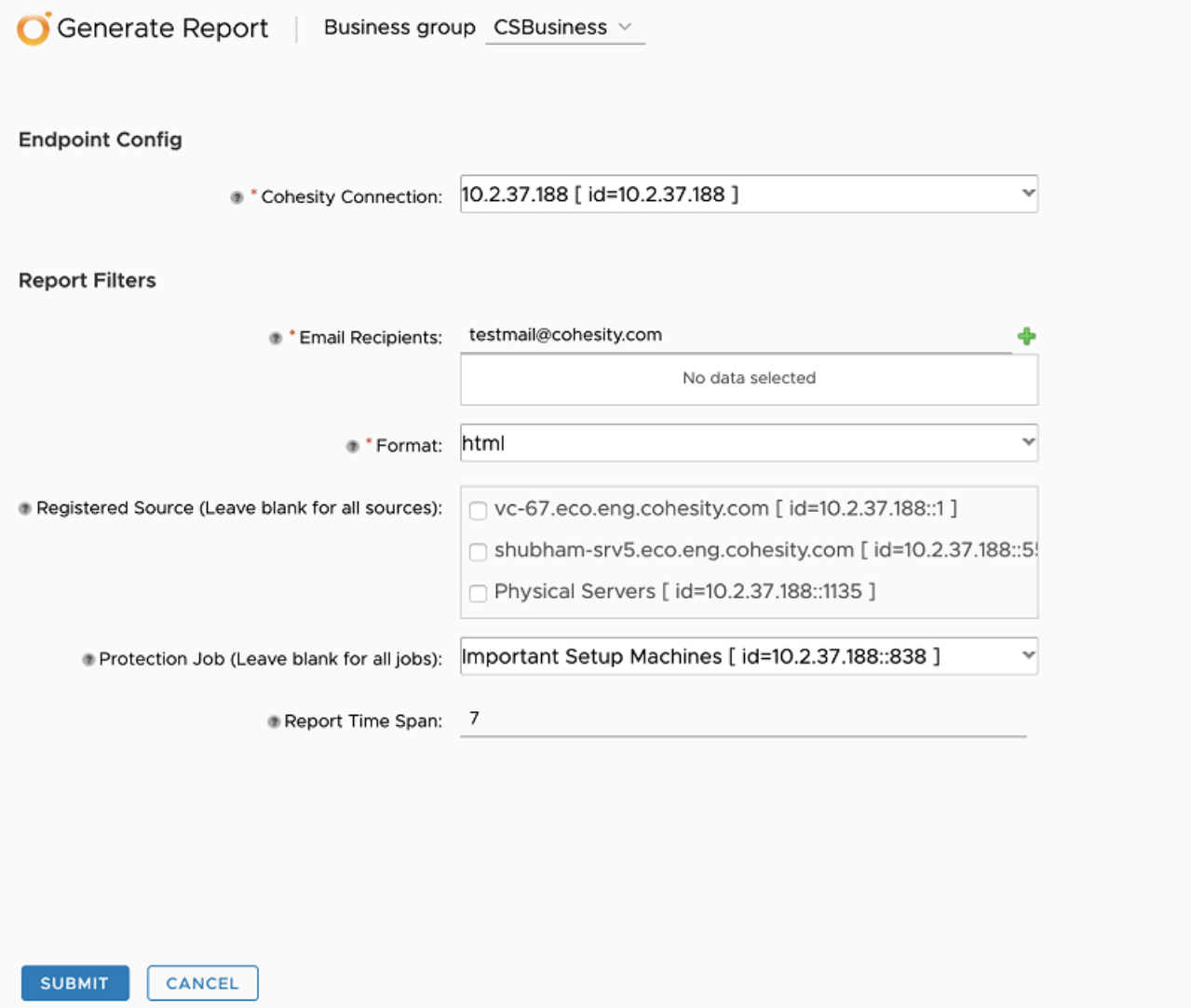
Procedure (XAAS)

To generate a report that provides an overview of the Protection Groups:

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 Group or if left blank, all the Protection Groups 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.



8. Click **Submit**. On success, the report will be emailed to the specified Email ID.

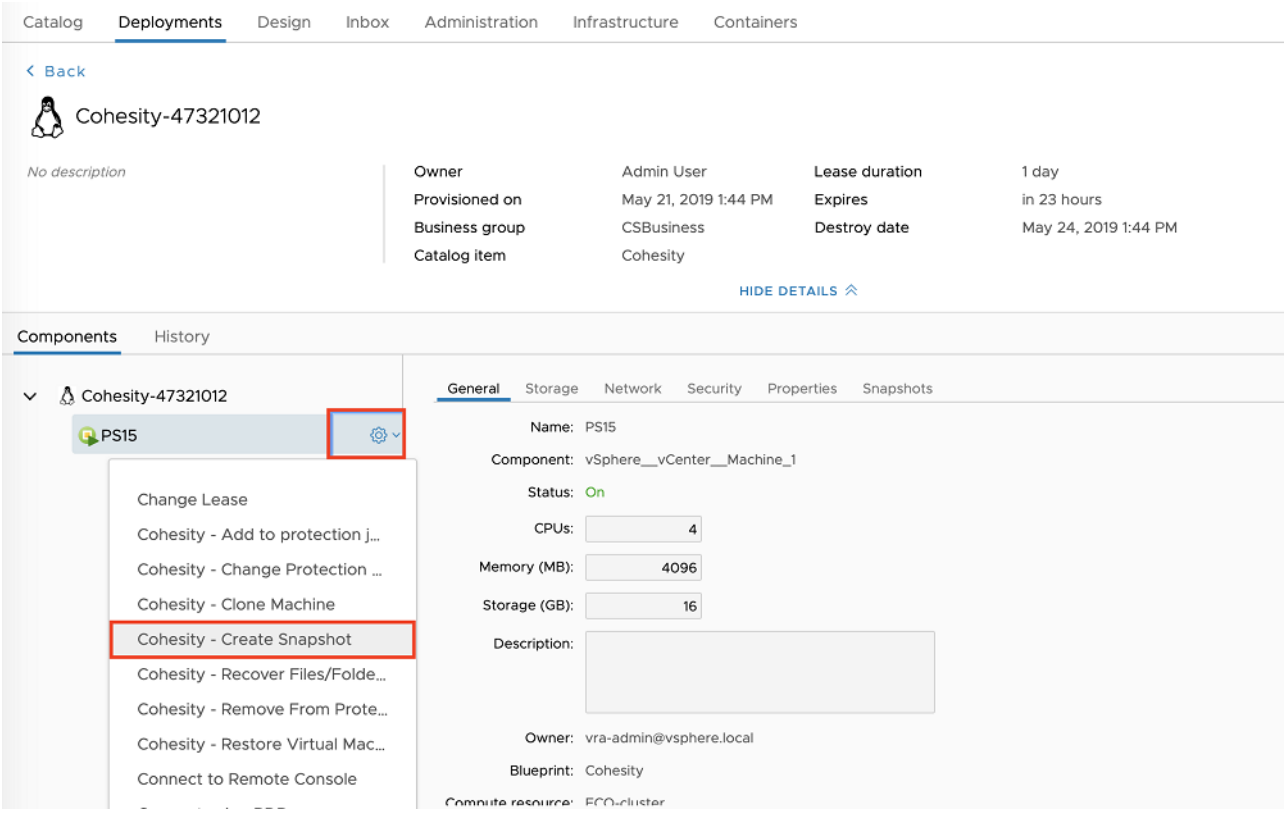
Executing a Protection Group on Demand as Resource Action

Procedure (Resource Action)

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

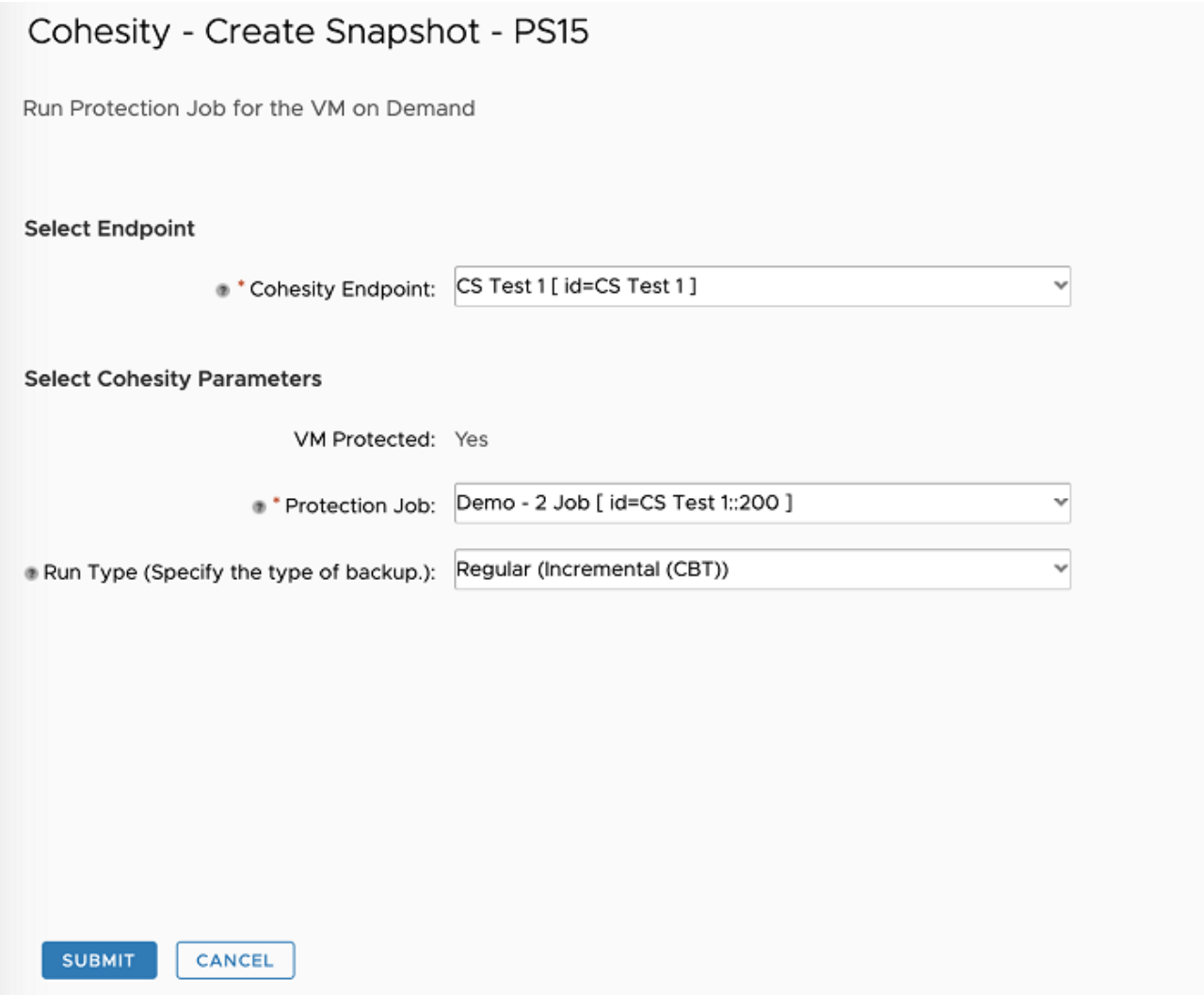
1. In the **Deployments** tab , click on the required provisioned VM.
2. In the **Components** pane in the bottom left of the screen, click on **Actions** icon (as highlighted in the figure).

3. Select **Cohesity-Create Snapshot**.



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 Group first.
6. In the **Protection Group** field, enter the Protection Group you want to execute.

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



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

Cohesity Enable or 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 for the Cohesity vRO plugin.

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**. On success, this will create a new Cohesity organisation and will bind the vRA tenant to the newly created organization.

Map vRA Tenant to existing Cohesity Org

Procedure

To map a vRA tenant to an existing 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.

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
Removing a Cohesity Endpoint	This section describes the details to remove an existing Endpoint.
Updating a Cohesity Endpoint	This section describes the details to update a Cohesity Endpoint.
Removing Email Configuration	This section describes the details to remove the Email configuration.
Updating Cohesity Email Configuration	This section describes the details to update an Email configuration.

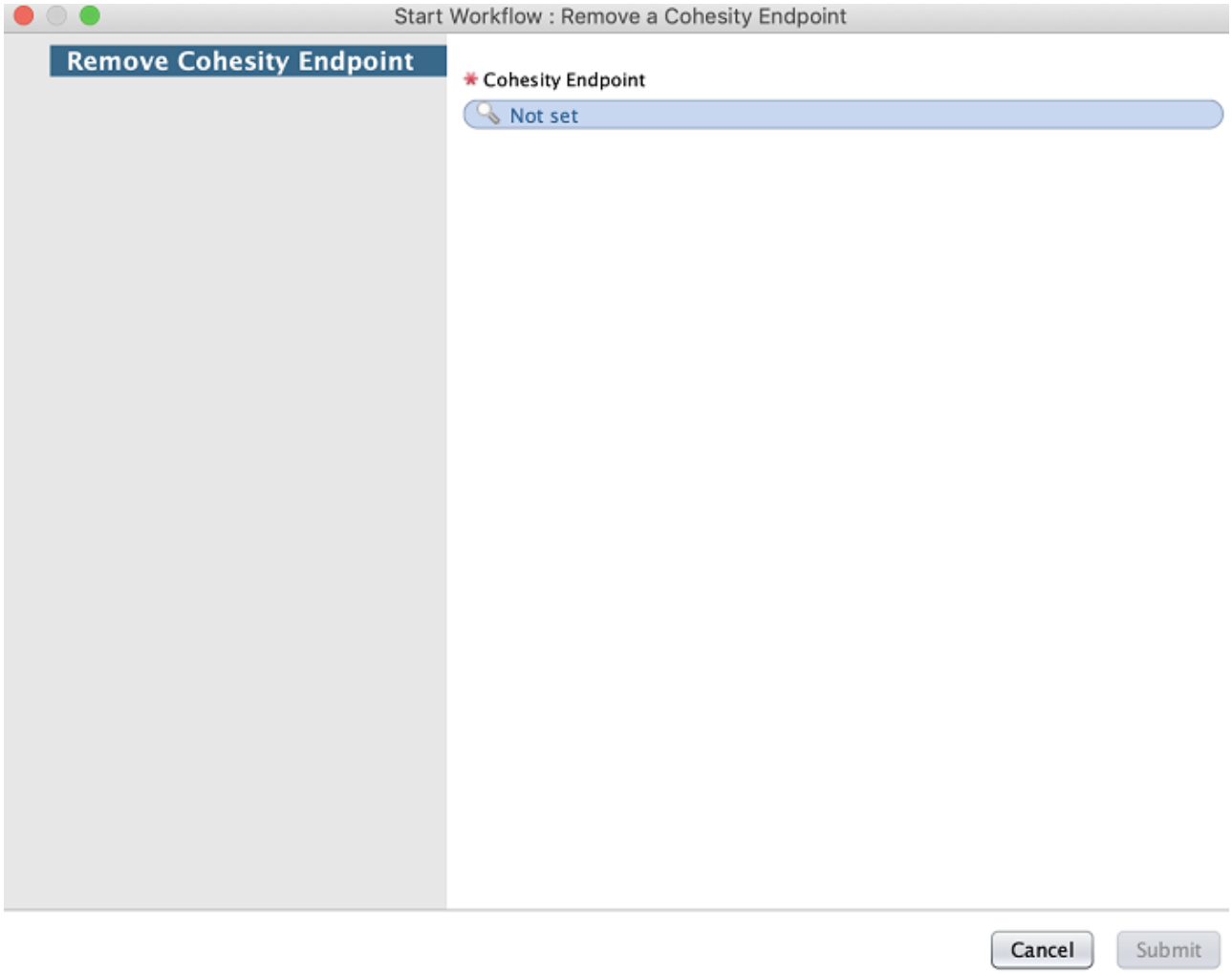
Removing a Cohesity Endpoint

Procedure

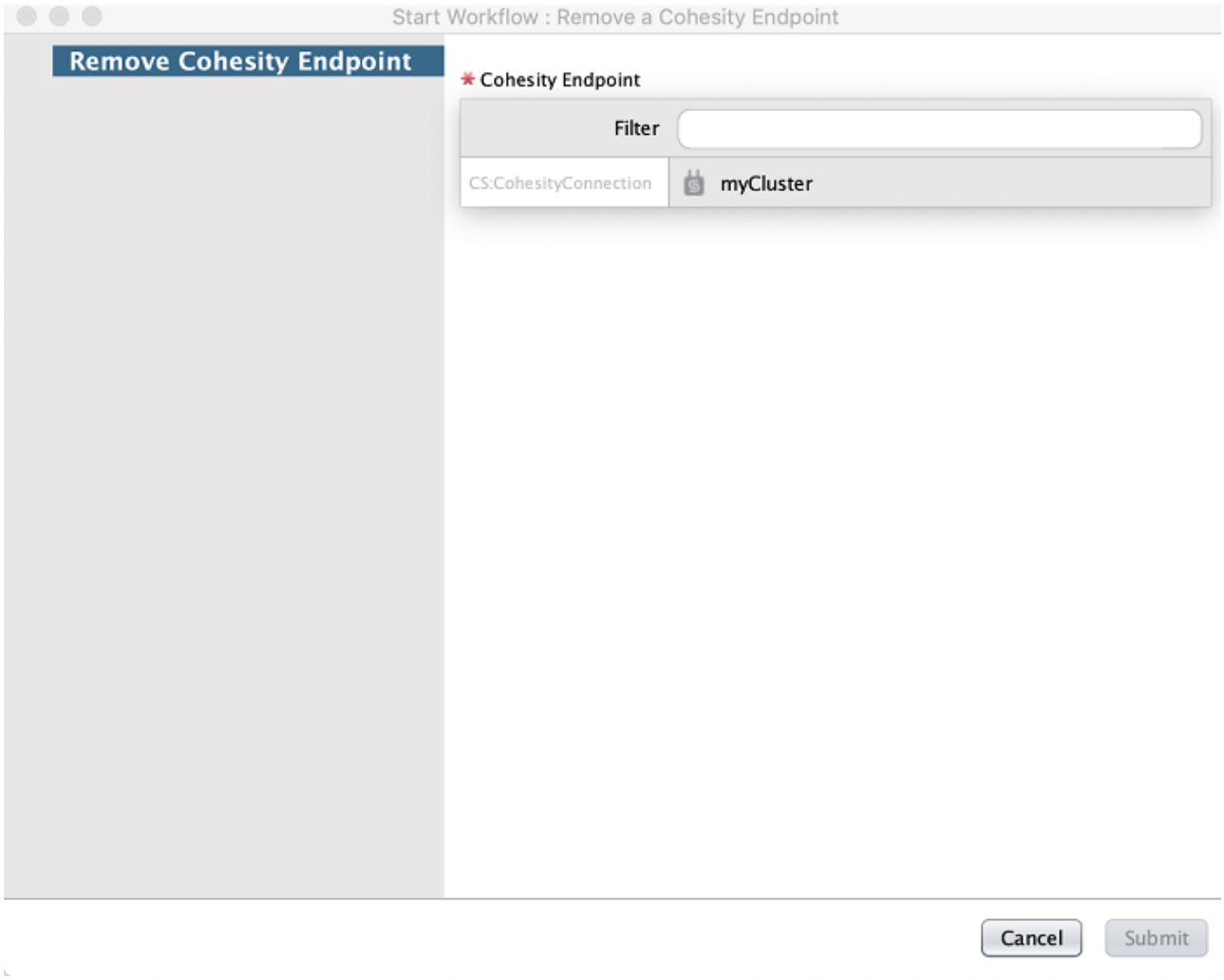
To remove an endpoint:

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**.

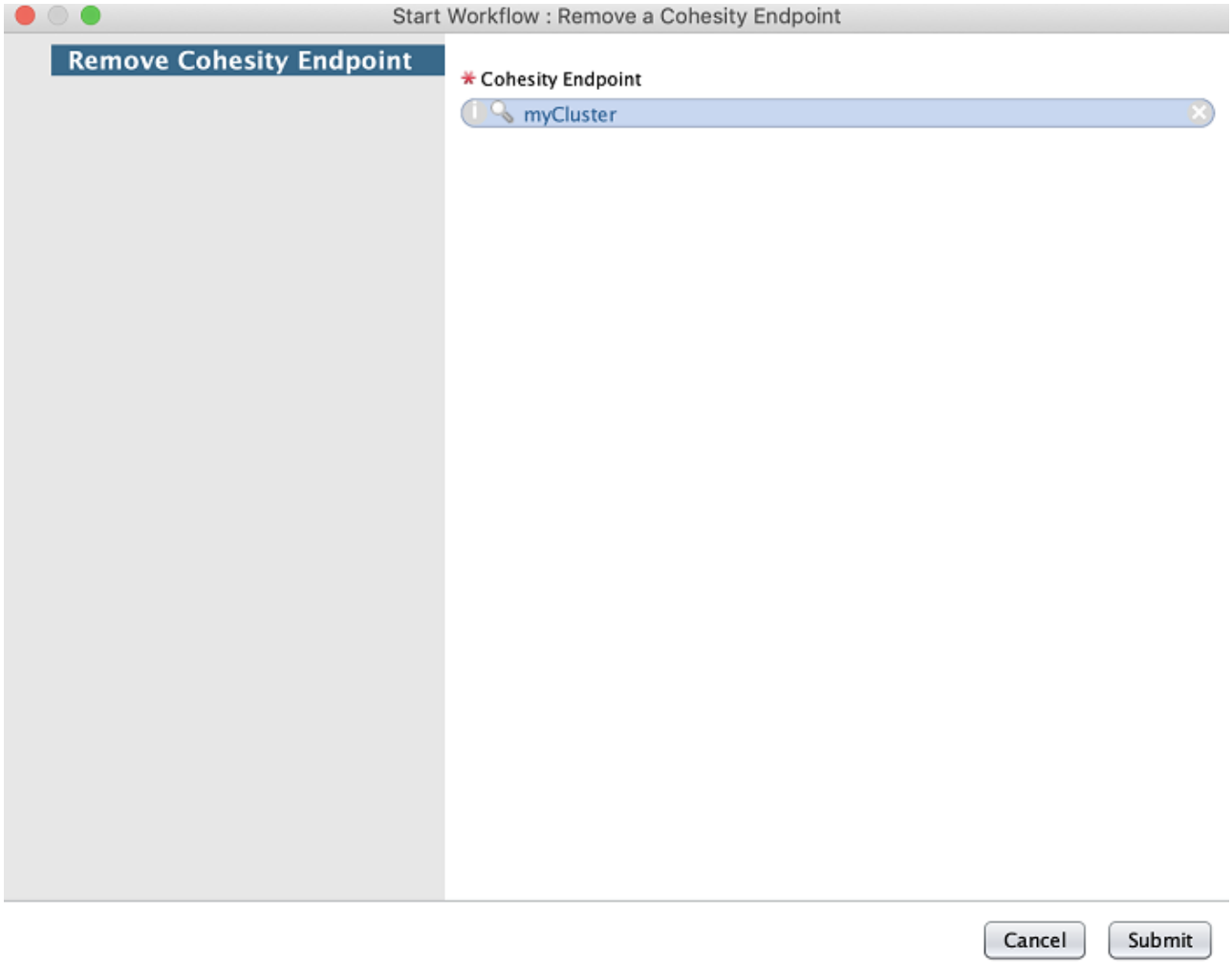
4. To start the workflow, click  . The **Remove a Cohesity Endpoint** screen is displayed.



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

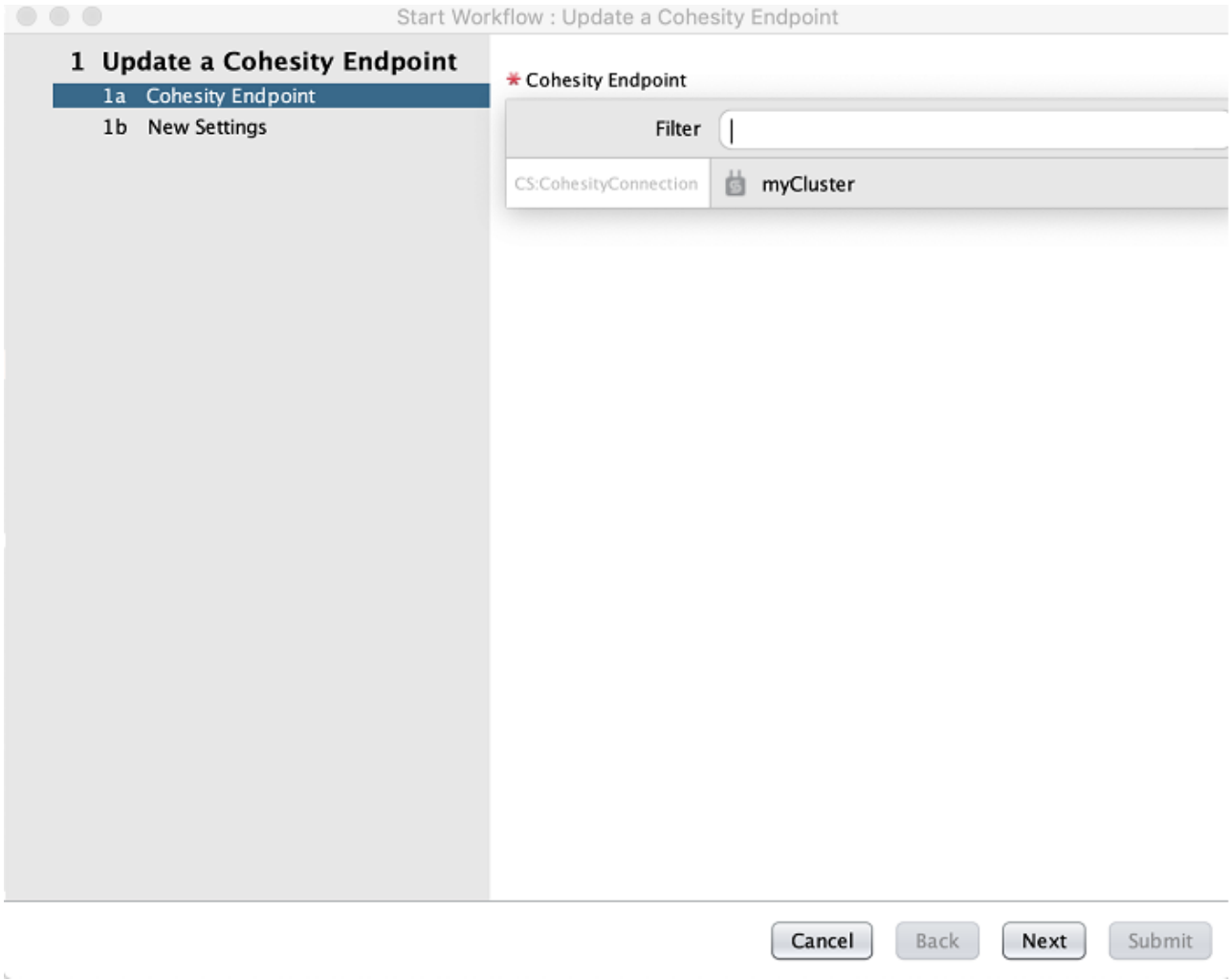
Procedure

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**.

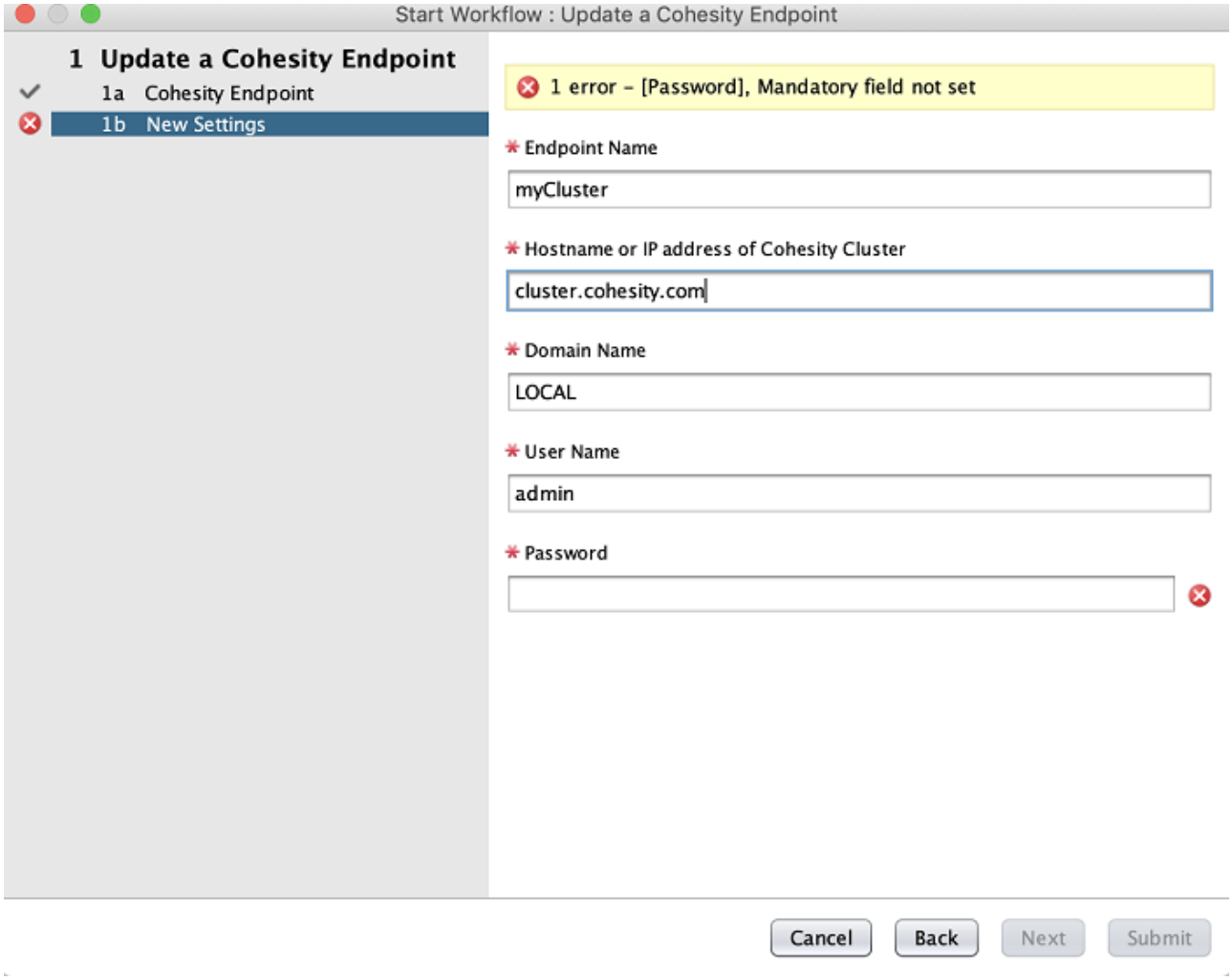
4. To start the workflow, click  . The **Update a Cohesity Endpoint** screen is displayed.

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



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**.



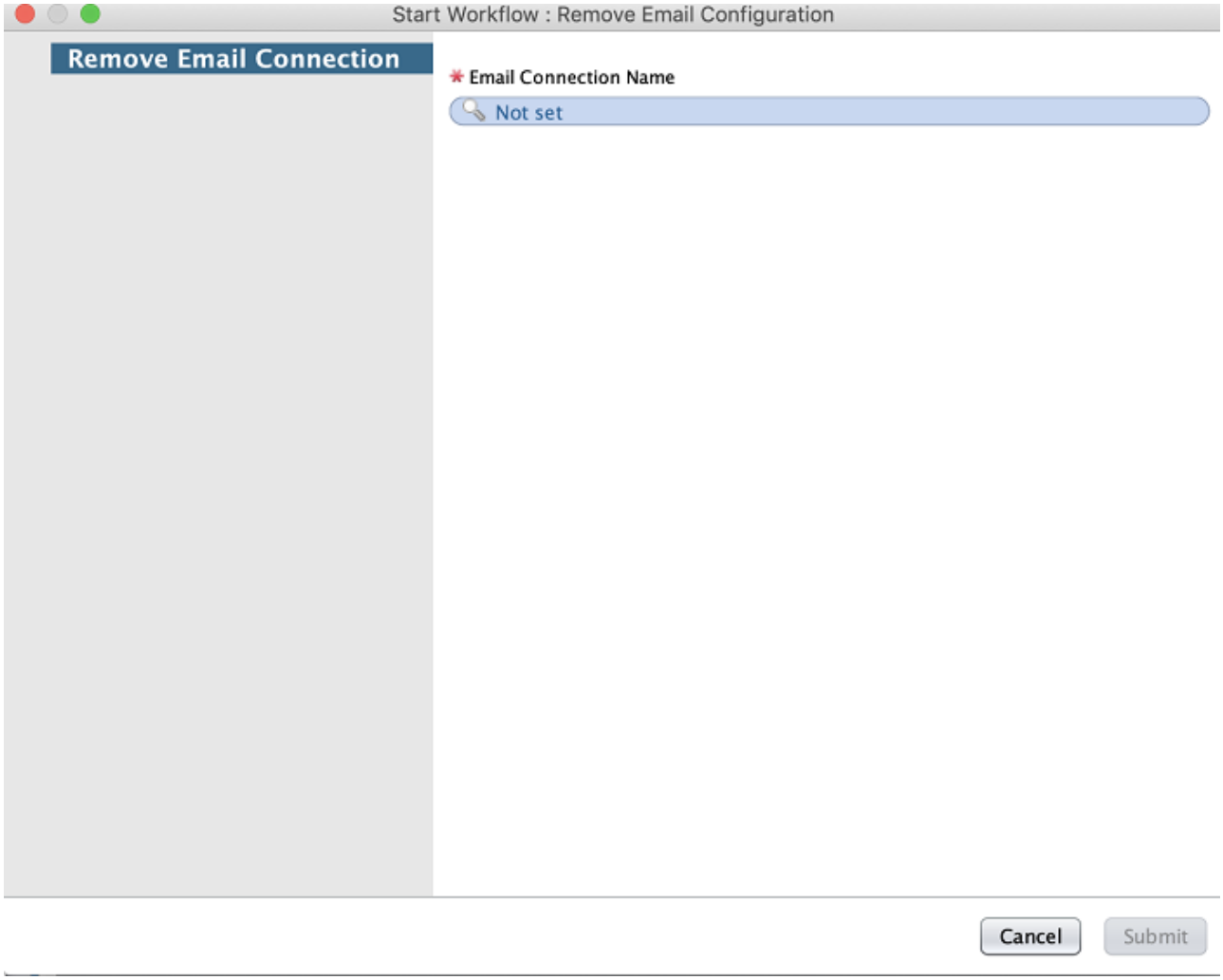
Removing Email Configuration

Procedure

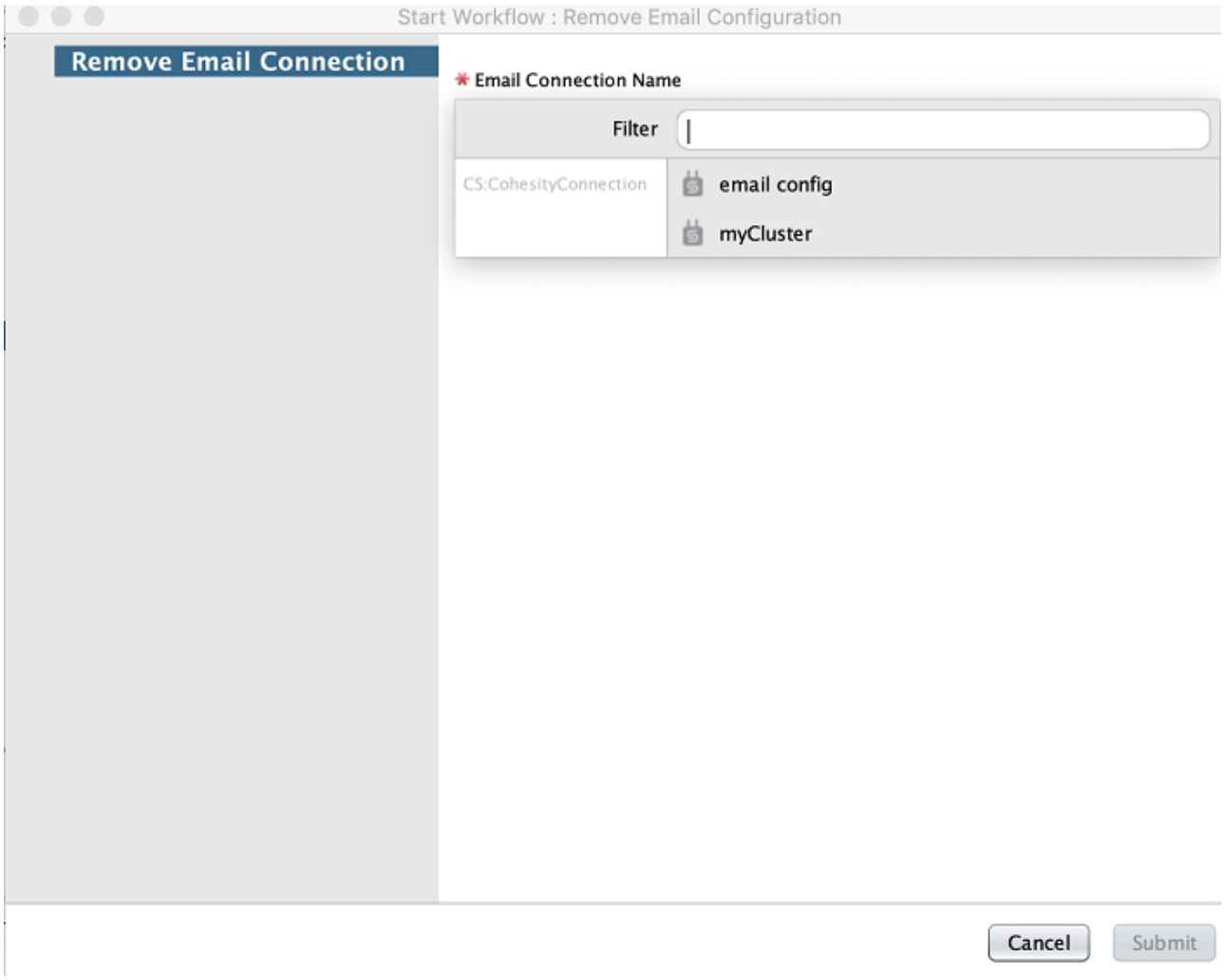
To remove Email configuration:

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.



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.



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

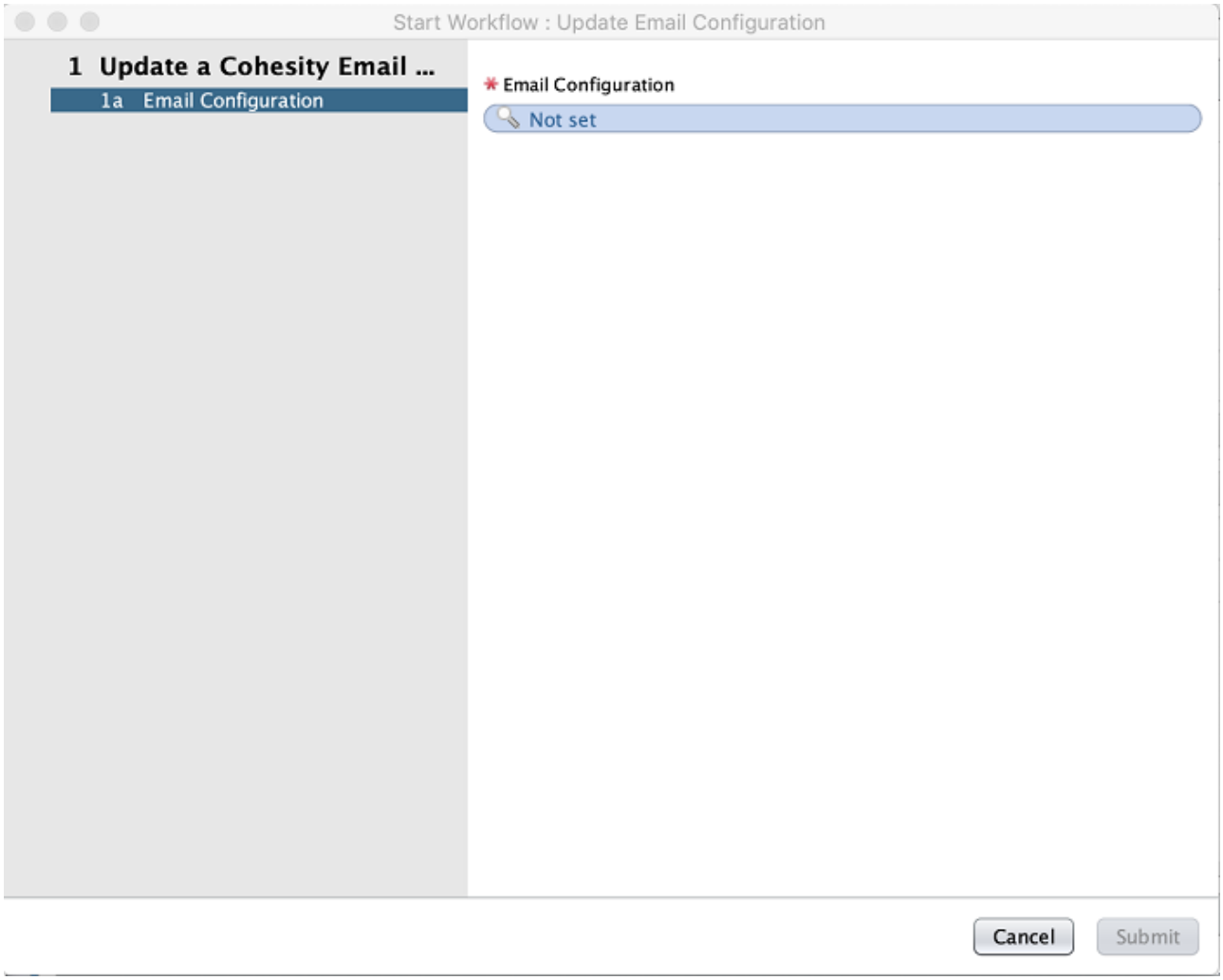
Updating Cohesity Email Configuration

Procedure

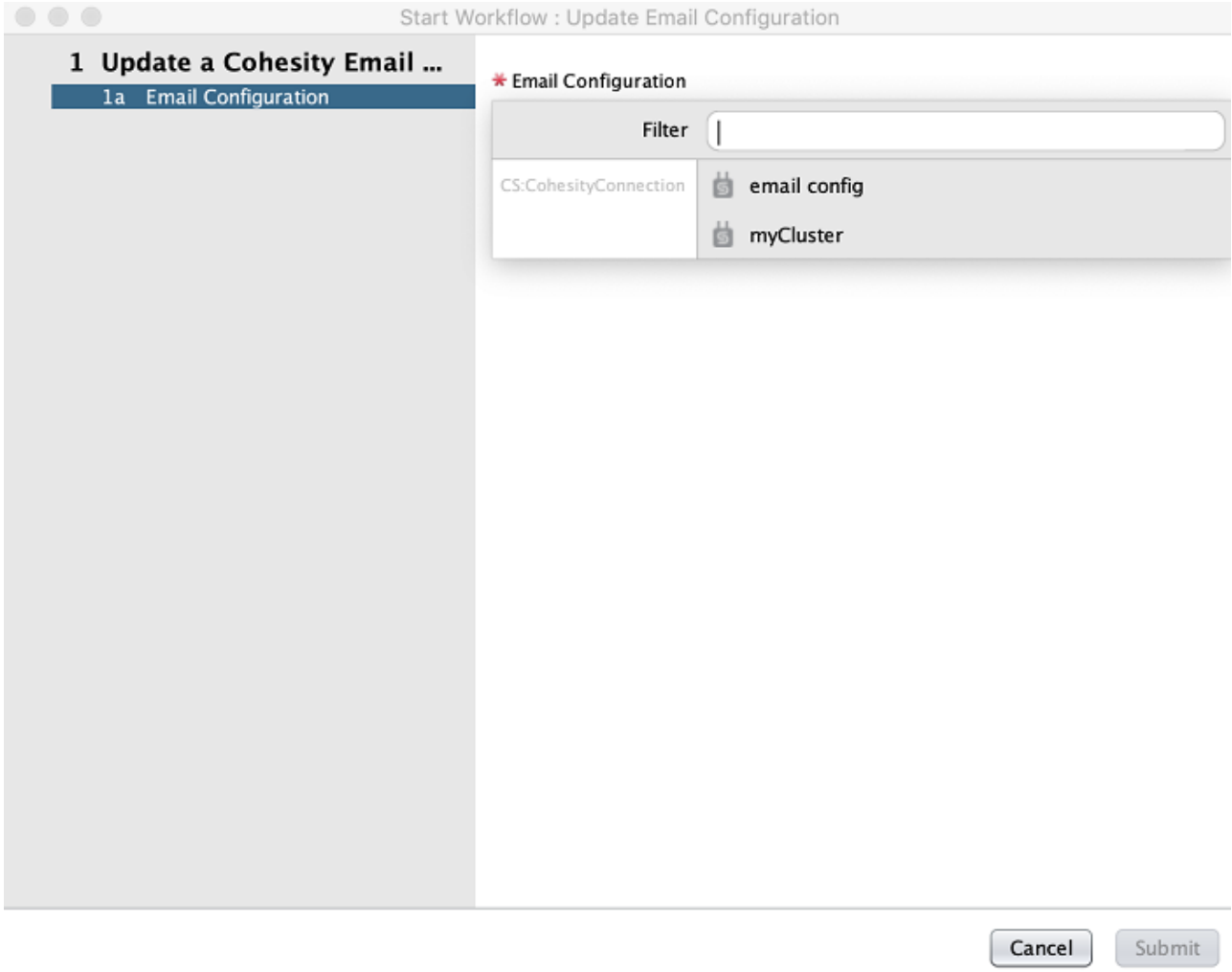
To update an Email configuration:

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.



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.



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**.