COHESITY

Protect VMware Cloud Director Multi-Tenant Environment with Cohesity

Cohesity Leverages VCD to Simplify Multi-Tenant Data Protection for Service Providers

Version 2.2

April 2026

ABSTRACT

In today's digital-first world, organizations and enterprises use VMware Cloud Director (VCD), a VMware offering to host multiple customers under one hardware layer and VMware Cloud Director (VCD) to provide seamless virtualized infrastructure as a service for multiple tenants. To protect that infrastructure efficiently and reliably, use these recommendations and best practices and configure Cohesity data protection for VMware Cloud Director (VCD), focusing on an efficient recovery strategy to extend the infrastructure as a service (IaaS) experience for service providers and tenants by going beyond surface-level protection. Cohesity recognizes its constructs and provides protection and recovery at the VCD, Organization, and even the vApp levels.

Table of Contents

Figures

Service Provider and Organization Overview

The service provider has two personas: the service provider's admin and Organizations (generally called Tenants). The service provider manages the tenants and provides services such as Infrastructure, platform, and software.

As service provider businesses expand, managing the growing number of tenant customers becomes more challenging. VMware Cloud Director (VCD) is a leading cloud service delivery platform that some of the world's most popular cloud providers use to operate and manage successful cloud service businesses. Cloud providers use VMware Cloud Director to deliver secure, efficient, and elastic cloud resources worldwide to thousands of enterprises and IT teams.

In this emerging infrastructure, multi-tenancy refers to the mode of software operation where multiple independent instances of one or multiple applications operate on shared hardware. The organizations are logically isolated but reside on the same physical infrastructure.

Customers are leveraging shared hardware in multi-tenancy, which reduces the cost of IT infrastructure. Customers are also leveraging it as a service model at a lower cost. Scaling a Multi-tenant environment has far fewer infrastructure implications for vendors. These advantages make onboarding new customers easy and seamless.

Given the number of tenants using their services, service providers are especially interested in keeping everything running reliably and smoothly. Another advantage of a multi-tenant environment is ongoing software maintenance and upgrades — their end-users don't need to pay costly maintenance fees to keep their software up-to-date.

The challenge is managing all these tenants in an automated, consistent, and secure way.

Today's Challenge: Managing and Mapping Multiple Organizations (Tenants)

Service providers greatly benefit from shared infrastructure, cost, and revenue. The advantages of a multi-tenant environment come with some predefined challenges, as

1. Data isolation and Data security
2. Ease of managing multiple Tenants
3. Authentication and authorization
4. Mapping or organization with other Applications

Every application integrated with the VCD, or multi-tenant services must follow the above best practices to be tightly intact with the VCD. To follow the data isolation between the customers, to demystify as Customer A is only able to see Customer A data, not Customer B. So, the third-party application must be multi-tenant and intact with the mapping, authentication, authorization, and isolation to not expose the customer data to each other.

Simplicity Meets Multi-Tenancy - Cohesity Seamless Multi-Tenancy

Cohesity Offers the simplest way to securely Manage, Map, and configure the VCD multi-tenancy with Cohesity. One of Cohesity's primary values for service providers is simplifying complex multi-tenant environments. Cohesity helps you simplify your data silos so you can focus on delivering superior customer experiences. Cohesity modernizes service providers' architecture and provides inherent hybrid connectivity for service providers to offer Backup as a Service (BaaS).

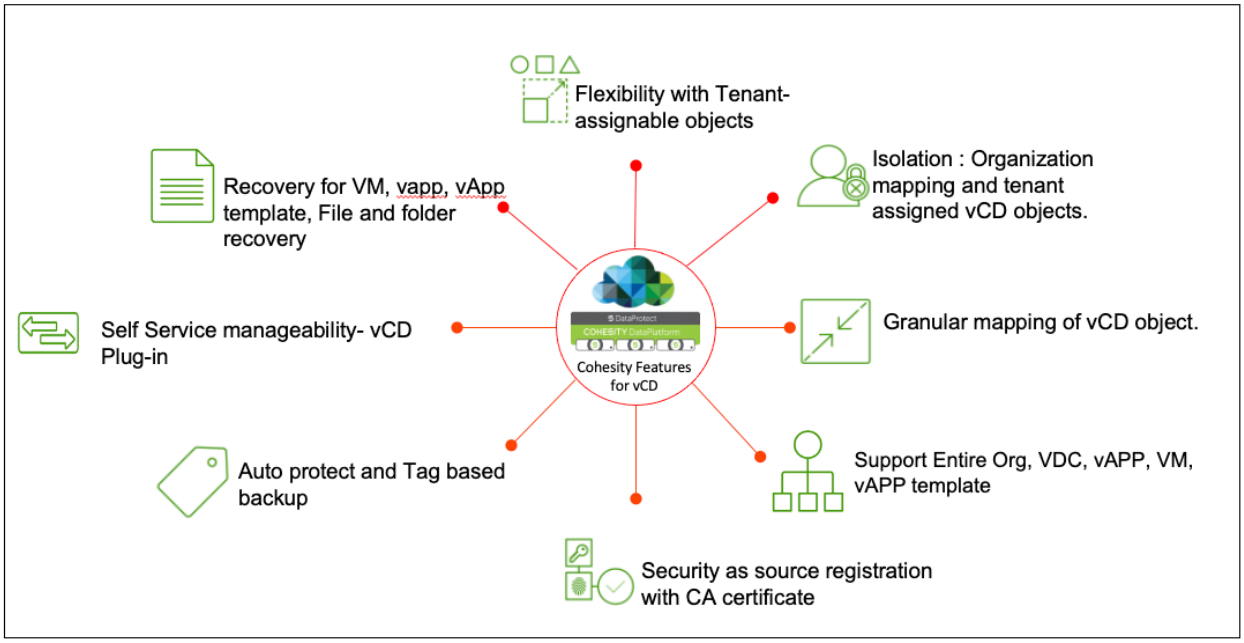
Cohesity's multi-tenancy capabilities enable you to:

- Configure multi-tenant environments on the Cohesity platform and securely isolate each tenant in your environment.
- Use a single/multiple Cohesity cluster to provide service to many tenants.
- Helios SaaS Platform as a single pane of glass to manage multi-tenancy.
- Support multiple customers' backups and workloads on the same platform with secure namespace isolation and per-tenant encryption.

With Cohesity's additional multi-tenancy features, this granular level of data protection enables tenant self-service capabilities for data protection, which lowers operating costs. Cohesity offers the following features with VCD:

NOTE: For more, see Organizations (Multitenancy) in the online Help.

Figure 1: Cohesity Features for VCD



Understand Different User Personas

Typically, two different types of users deploy this solution: Service Providers (SPs) and Organizations (Tenants). It is important to understand how the workflow for each user type differs.

Service Provider

A Service Provider (SP) provides Infrastructure-as-a-Service (IaaS) and other services to its organizations or tenants. An SP has to manage hundreds of thousands of organizations and ensure that each Organization is isolated from the others and that data and resources cannot be visible or cross from one Organization to another. VMware Cloud Director (VCD) helps an SP provide this separation among organizations using VMware's VCD Organization construct.

Cohesity's multi-tenancy solution allows the SPs to map their VCD Organizations (aka tenants) to Cohesity Organizations. This way, SP can offer self-serviced Data Protection services to its tenants via Cohesity Organizations. To do that, the SP must register the VCD on Cohesity, create Cohesity Organizations, and map them to the VCD Organization. Only service providers can manage the creation of Cohesity Organizations. Their tenants can then log in using the Cohesity Organization's credentials to protect their data.

Organization (Tenant)

A tenant is an enterprise or small-to-medium business to which the service provider caters. Each tenant is mapped to a Cohesity Organization, on which the tenant can access only the resources assigned to them. This ensures tenants do not have access to other tenants' data and provides a logical separation, giving a completely independent view of the Cohesity.

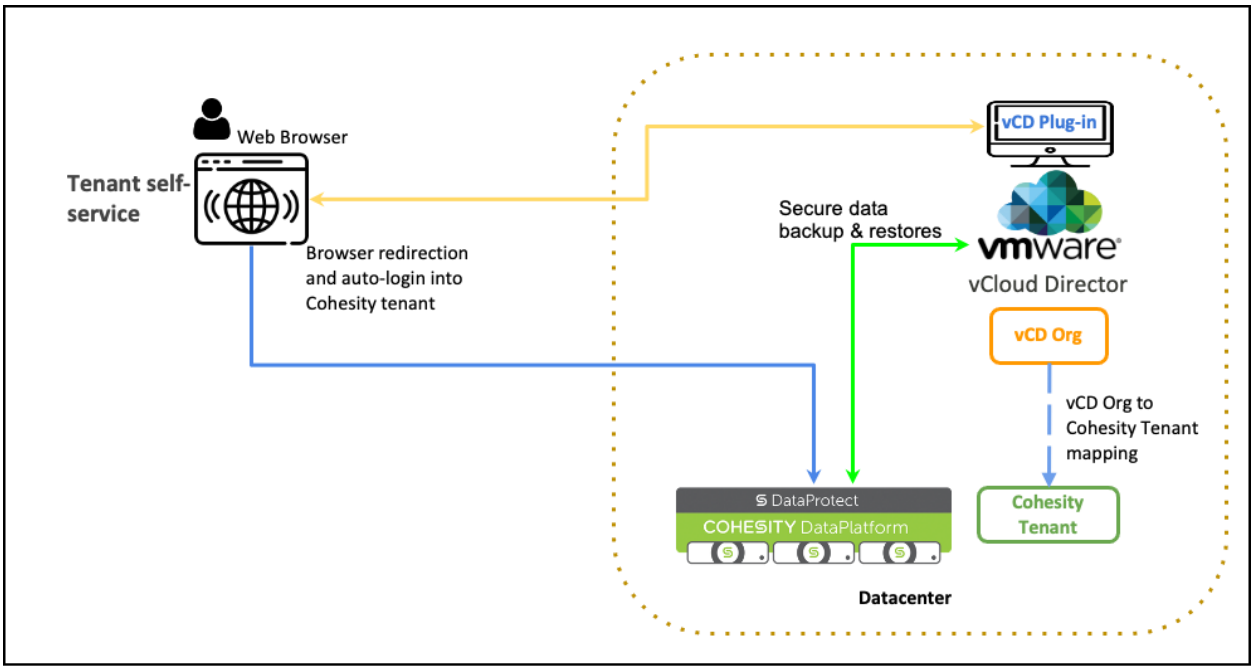
Protect VMWare Cloud Director

The Cohesity platform is designed to integrate with VMware Cloud Director, recognizing its constructs and providing protection and recovery for:

- VMware Cloud Director
- VCD Organizations (vOrgs)
- Virtual data centers (vDCs)
- vApps (including the VMs that comprise them)
- Standalone VMs
- Template's

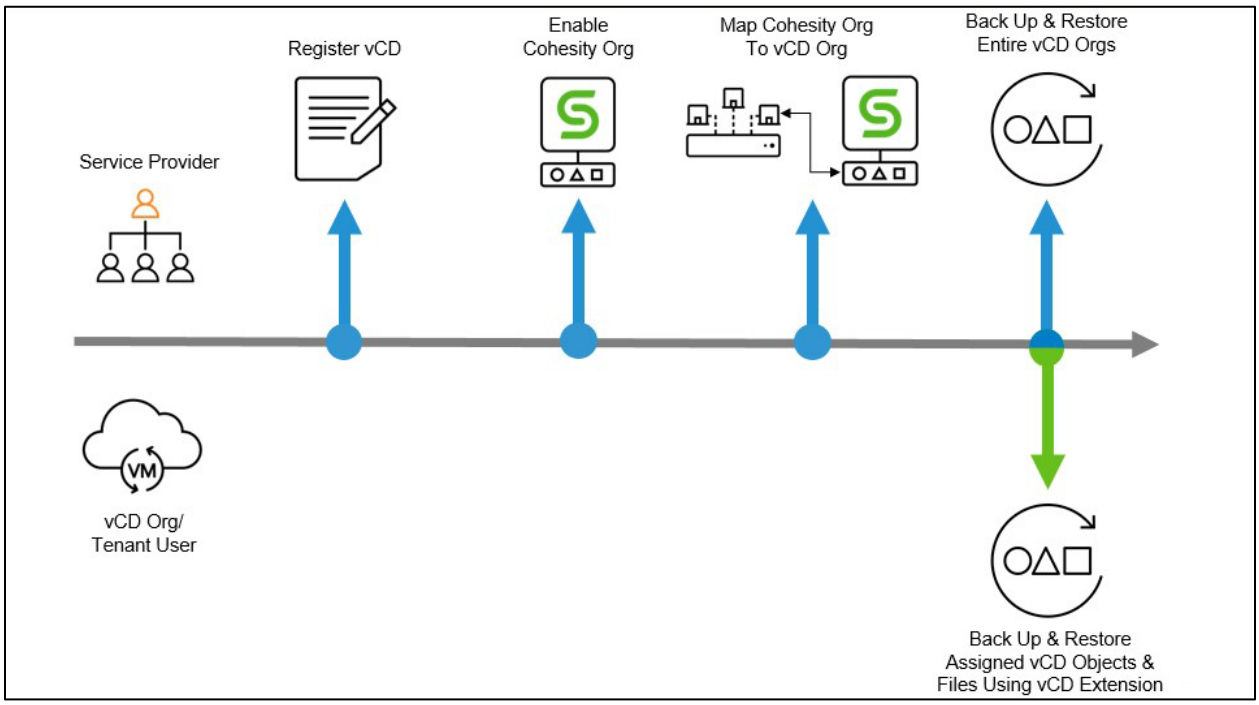
Cohesity provides flexibility to protect the VCD environment from both the personas of service providers and organization users. For VCD organization users to protect resources, multi-tenancy must be enabled on Cohesity, and the provider must map the VCD organization to a Cohesity organization. The final solution will be as follows.

Figure 2: The Final Solution



To protect the VCD environment, the service provider and organization user must follow three basic steps: Enable Multi-tenancy on the Cohesity cluster, Register the VCD resources, and create and map organizations.

Figure 3: Set Up Cohesity Protection for VCD



NOTE: To familiarize yourself with the key terms and concepts that constitute this solution, see Appendix A: Terminology.

To set up Cohesity protection for your VCD sources:

1. **Enable Multi-Tenancy.** The service provider user must enable multi-tenancy by enabling Organizations on the Cohesity Cluster.
2. **Register your VCD Source.** The service provider will register the VCD source on the Cohesity cluster.

   NOTE: As a service provider, you can also set up protection for the VCD source you just registered. That will enable you to recover the VCD source and its objects.
3. **Create and Map Organizations.** Before protecting the VCD organization source and its object, the service provider user must create the Cohesity organization and map the VCD organization or its object to the Cohesity Organization.
4. **Protect VCD Resources**. To protect the VCD organization and its sources, VCD organization users can access the mapped objects in the form of Organization, VM, vAPP, and template. The next step is to create or use the existing protection group. It can be set up by the Service provider or organization user for the registered and mapped objects.
   a. Register new protection sources.
   b. Protect registered sources.
   c. Recover protected sources.

NOTE: As a self-service model, VCD Organization users can also use Cohesity's VCD plugin to protect and recover their VCD resources.

Register VCD as Source

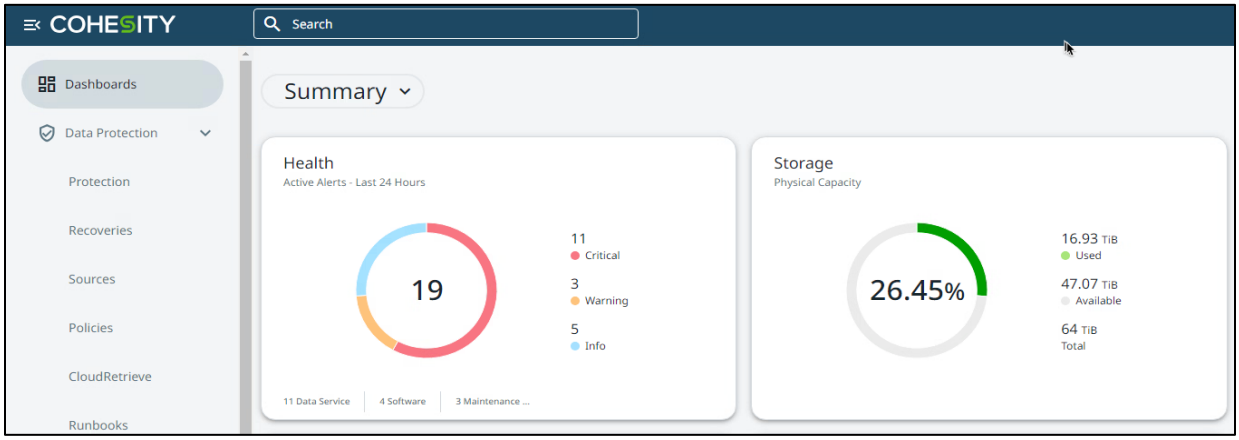
Registering VMware Cloud Director with Cohesity is a simple and two-step process to set up granular and SLA-based auto protection by entering the VCD Hostname or IP address and the appropriate credentials.

Registering a VCD environment is similar to connecting and authenticating the individual vCenters you have under management. Before registering, make sure you meet the following prerequisites:

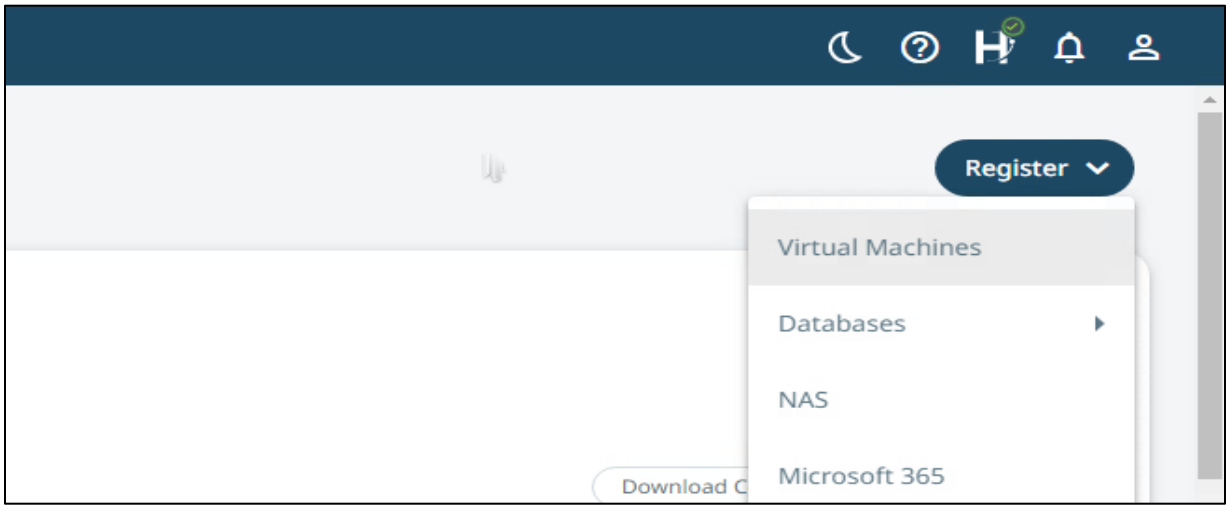
- Support Matrix
- Supported Version
- Minimum Permission

To connect a VCD environment:

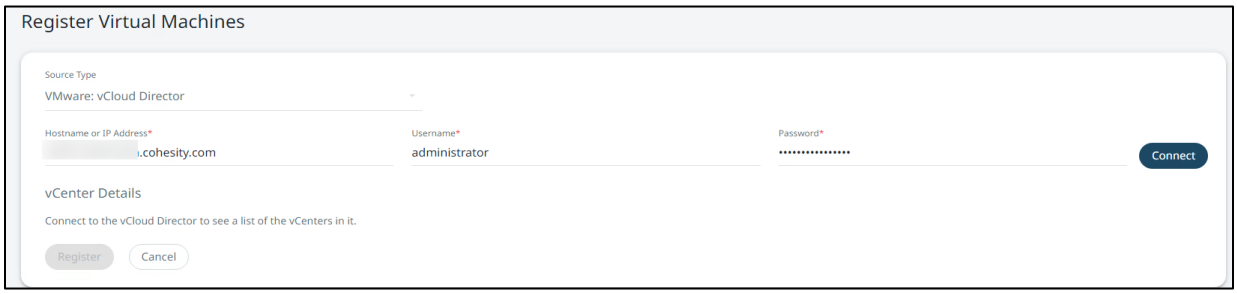
1. Log in to Cohesity and go to **Data Protection** > **Sources**.



2. Click **Register** and select **Virtual Machines**.

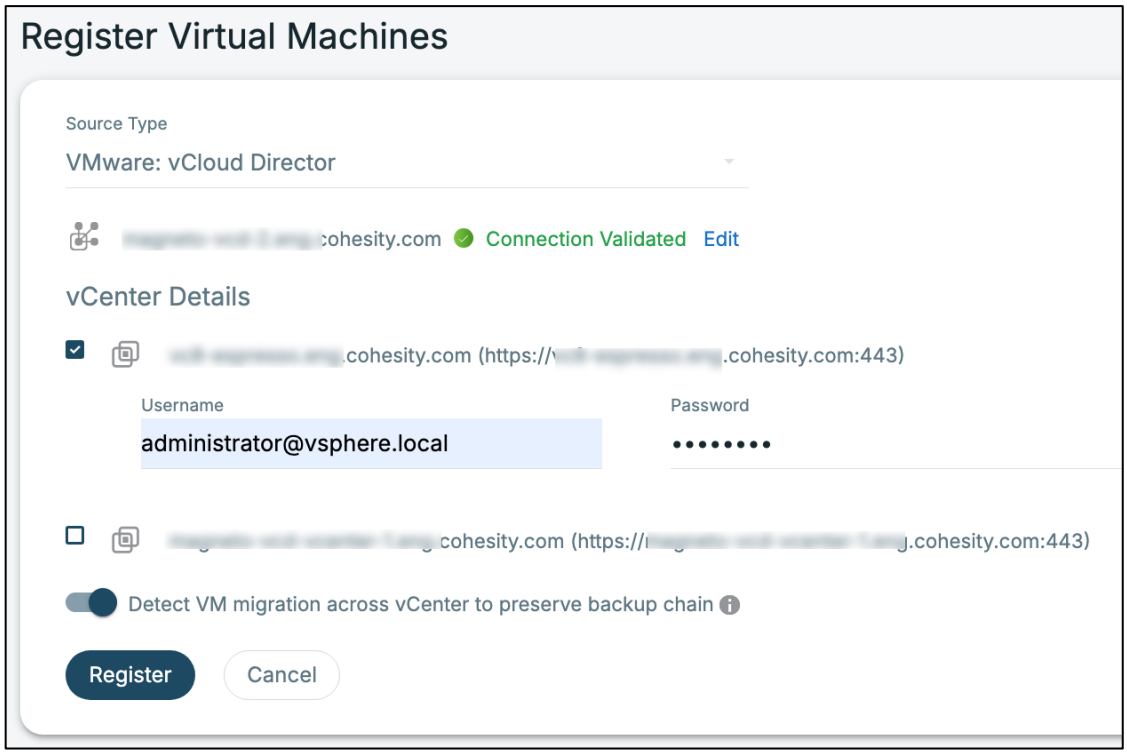


3. In **Source Type**, select **VMware**: **vCloud Director**, enter the **Hostname** or **IP address** with the credentials, and click **Connect**.



It will validate the credentials and display the discovered vCenter, which is part of the VCD infrastructure.

4. Select the vCenter you want to register and enter the vCenter credentials
5. If desired, enable option “Detect VM migration across vCenter to preserve backup chain” (available in release 7.3 and higher) and click **Register**.



NOTE: When you enable **“Detect VM migration across vCenter to preserve backup chain”**

- It enables Cohesity cluster to detect the VMs that are migrated from the current VMware vCenter to vCD.
- Cohesity cluster eliminates the need for a full backup of the migrated VMs as the VMs are protected before the migration. Only an incremental backup is needed.
- Cohesity will display “vCenter Migrated” against the VM in the “Add Object” page of the Protection Group creation workflow.

Create a Protection Group to Protect VCD Source

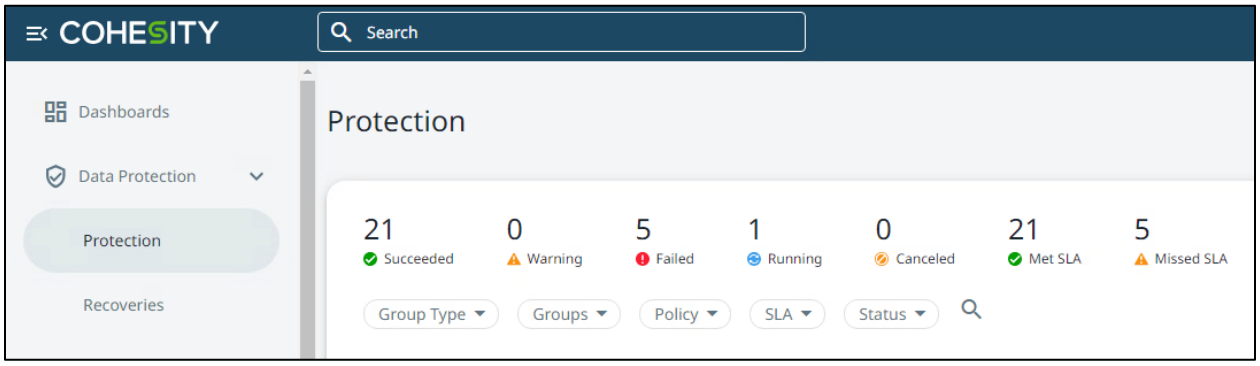
Cohesity provides granularity and flexibility to protect the VCD source or its individual objects, as mentioned below. Users can protect the VCD object at every level of VMware Cloud Director without enabling or mapping the sources with the Cohesity organization. Also, you can protect the VCD source by allowing multitenancy on the Cohesity Cluster and mapping the VCD organization with it. Refer to the Multitenancy section for more details.

- Entire VMware Cloud Director environments (*SPs*)
- Individual VCD Organizations (*SPs and tenants*)
- Virtual data centers (*SPs and tenants*)
- vApps & vApp templates (*SPs and tenants*)
- VMs within vApps & standalone virtual machines (*SPs and tenants*)

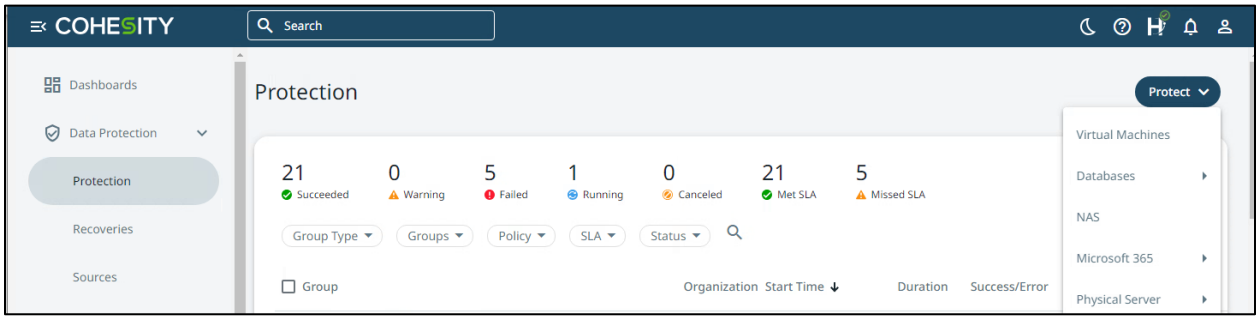
Data protection complements your multi-tenancy objectives by protecting VCD objects at different hierarchical levels; you can protect any Organization or virtual data center (vDC) as needed.

To create a Protection Group:

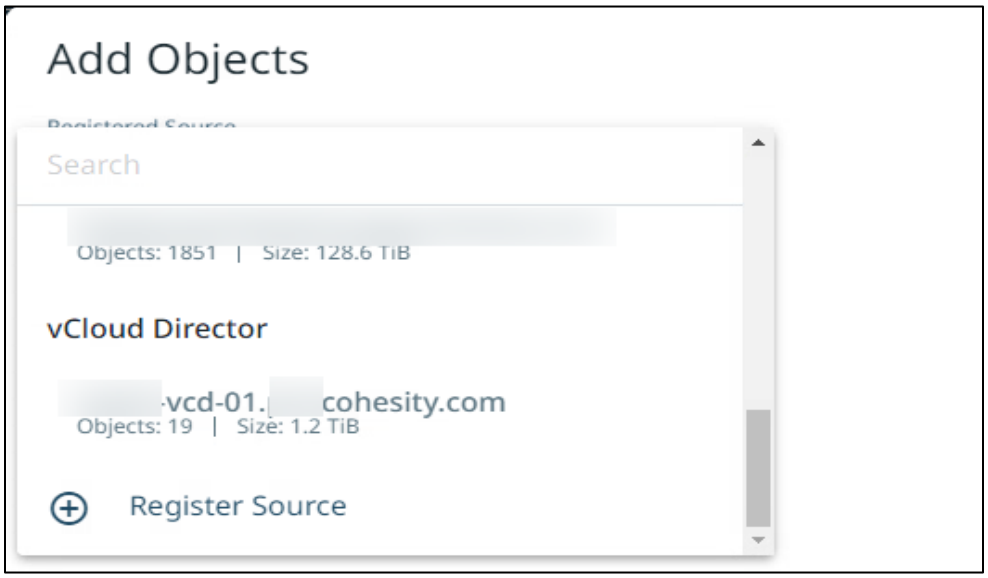
1. Log in to Cohesity and select **Data Protection** > **Protection**.



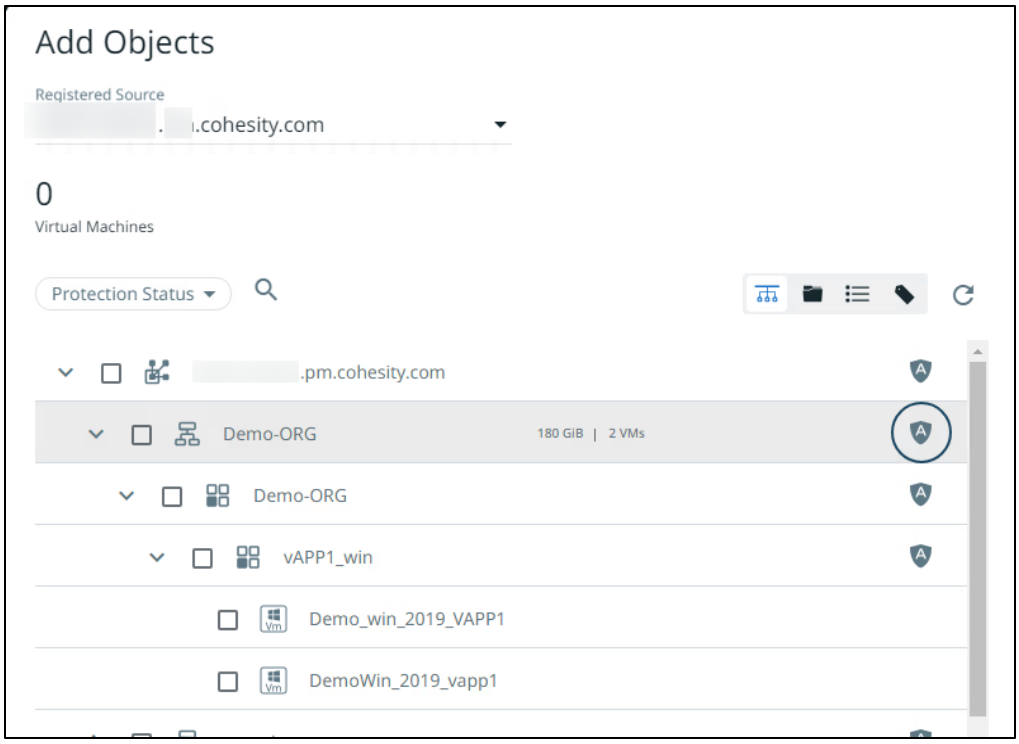
2. Click **Protect** and select **Virtual Machines**.



3. Add objects from the **Registered Source** and select the VCD environment under **vCloud Director** that you registered in the previous step.



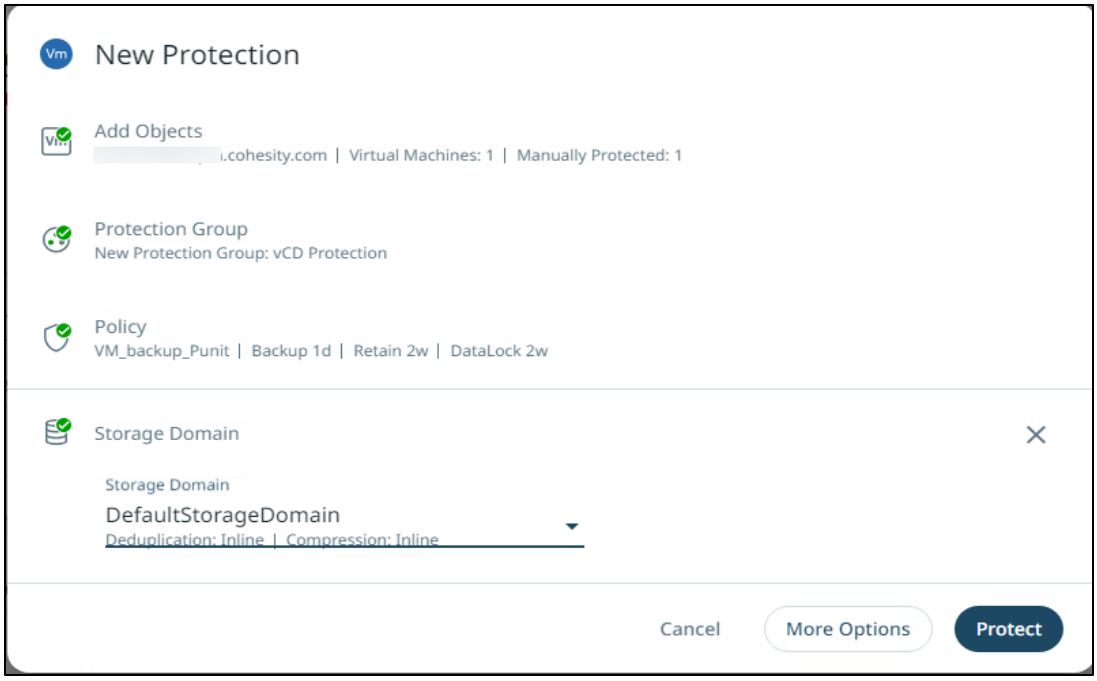
4. Select the VCD objects (VCD organization, vAPPs, vAPPs template, and VMs) to protect, click the shield icon on the right to enable Auto Protect, and then click **Continue**.



You can select entire VCD Organizations, virtual data centers (vDCs), vApps, VMs under vApps, or individual VMs to protect. Cohesity allows selecting the folder or tags as a parent object with its associated child. When applying Auto-Protect to a VCD object, Cohesity dynamically protects that object and any new child objects every time the Protection Group runs.

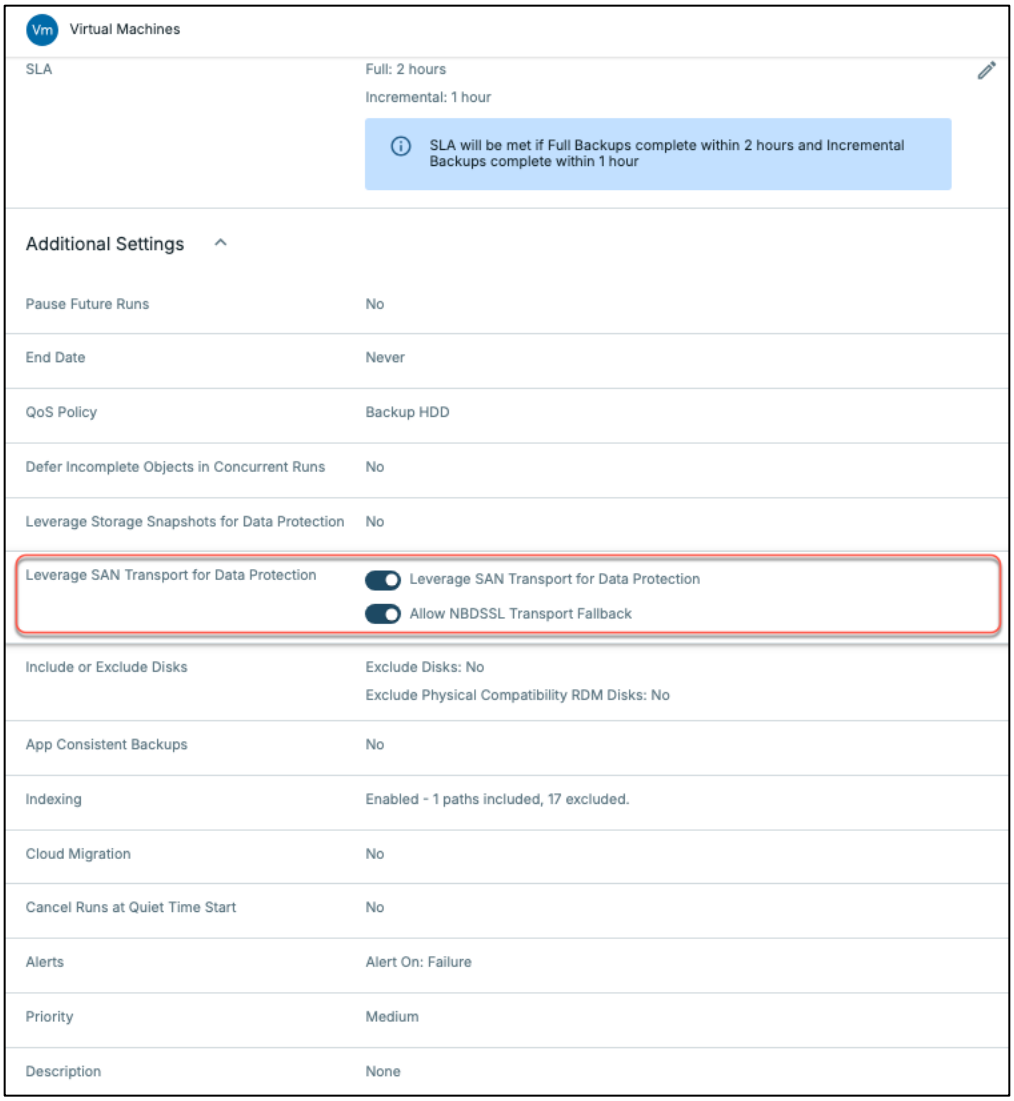
NOTE: You must use the Auto Protect option to protect a VAPP or VAPP Template should you wish to recover the VAPP or the VAPP Template.

5. Enter a **Name** for the Protection Group and select a **Protection Policy** of your choice.
6. Select a **Storage Domain** for this Protection Group.
7. Configure any **Additional Settings** that you need and click **Protect**.



Leverage SAN Transport Mode

In Additional settings, you can optionally leverage the SAN transport mode to run the backup over the SAN as FC/iSCSI. This feature will transfer the backup data from the VCD infrastructure to the Cohesity Cluster using the SAN mode, which benefits in faster backup and recovery. Kindly refer to the SAN transport for more information.



For details on the Additional Settings, see Add or Edit a Protection Group for Virtual Servers in the online Help.

NOTE: You can either choose to enable either “Leverage Storage Snapshots for Data Protection or Leverage SAN Transport for Data Protection” but not both.

Recover VMware Cloud Director Objects

Cohesity provides granular recovery, which enables you to recover vApps, Individual VMs, and vApps VMs. Users can choose the storage profiles and organization vDC networks for recovery.

Supported Recovery Workflows and Locations

Before you start, it is important to understand the specific recovery process that allows users to perform recovery on supported recovery locations. Due to the VMware architecture limitation, Cohesity will not allow you to recover the objects to the empty VCD organization. To recover the VCD object to the Empty VCD organization, you must create a dummy or empty vAPP.

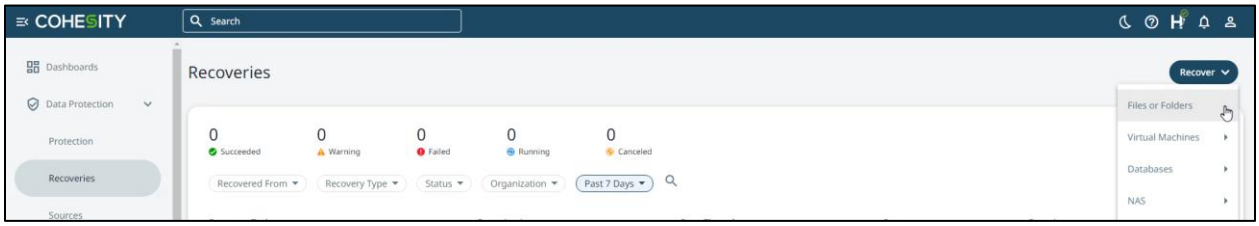
Object	Workflow	Supported Recovery locations	Supported Entity
VM	Backup, Archival and Replication	Original and Alternate	Original and alternative vApp, vDC, vCenter
VMDK		Original and Alternate	Original and alternative vApp, vDC
Files and Folders		Original and Alternate	Original and alternative vApp, vDC
vAPP		Original and Alternate	Original and Alternate vDC
vAPP Templates		Original and Alternate	Original and Alternate vDC

Recover Files and Folders

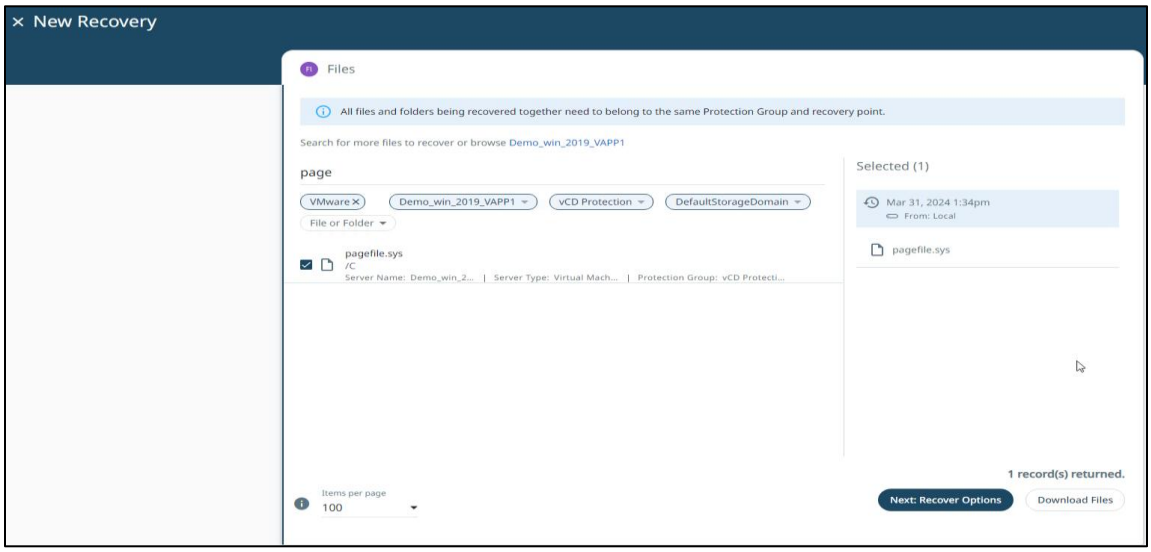
Cohesity allows you to search the files and folders within the virtual machines in VMware Cloud Director for granular data recovery. Follow the process below for granular recovery.

To recover specific files and folders:

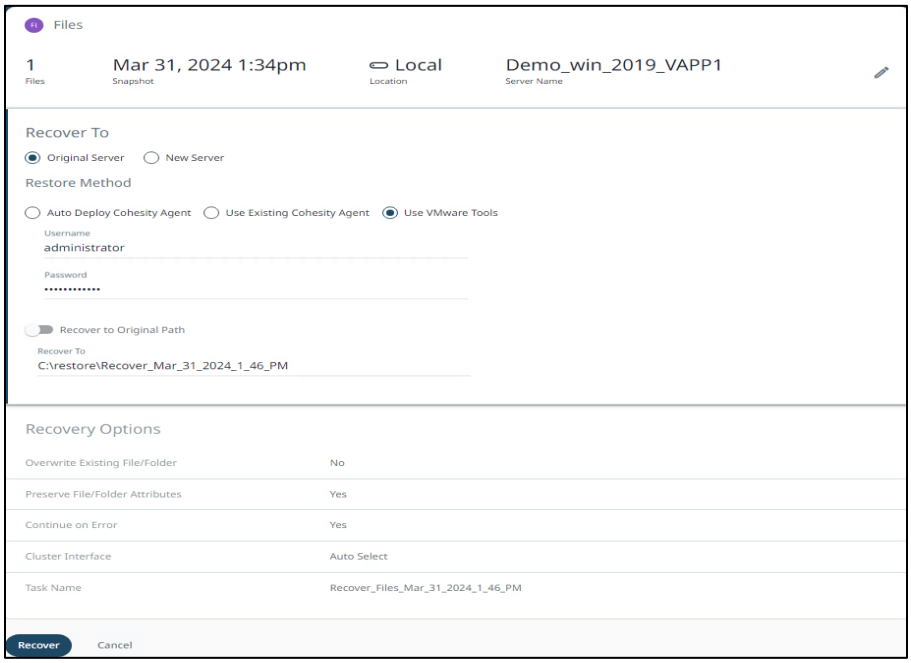
1. Log in to Cohesity and navigate to **Data Protection > Recoveries**, then click **Recover** and select **Files or Folders**.



2. Enter the filename or folder you need to recover or filter the object by selecting the Protection Group that includes it. You can use the '*' wildcard character to use partial names or to broaden your search. Use the filters to narrow your search. Select the file(s) that you want to recover. Under **Selected**, you can choose a different snapshot from which to recover. To continue, click **Next: Recover Options** or to download the file(s) directly, click **Download Files**.



3. Select whether to recover the file to the Original Server or New Server. Choose a **Restore Method**. You can select **Auto Deploy Cohesity Agent** or **Use VMware Tools**, enter the VM credentials. Configure the Recovery Options as required and click **Recover**. This creates a recovery task.



4. When the recovery task is completed successfully, the recovered file will be available in the specified location.

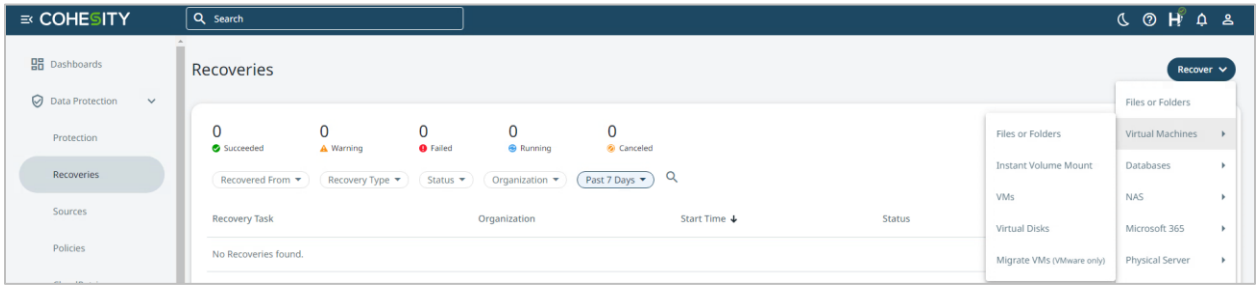
For more information on Files and Folders recovery and the Recovery Options, see Recovery Files or Folders in the online Help.

Recover VMs

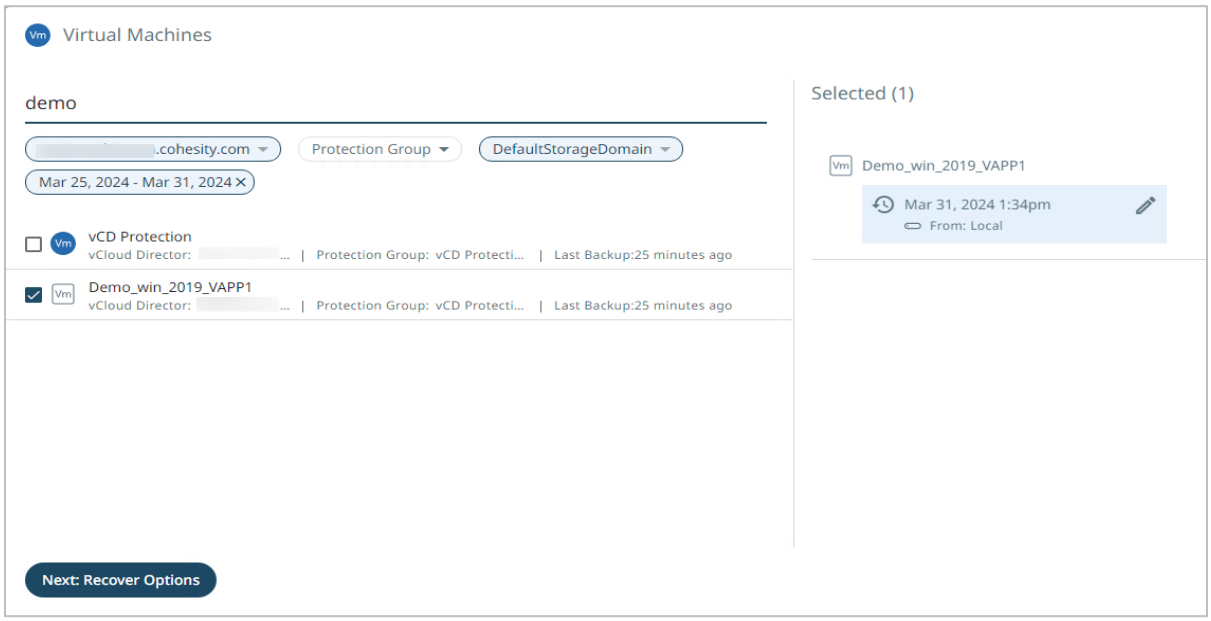
You can recover VMs to the same location or an alternate location, within a vApp or virtual data center with the same configuration, providing greater data protection capabilities to multi-tenant businesses like service providers.

To recover a VM:

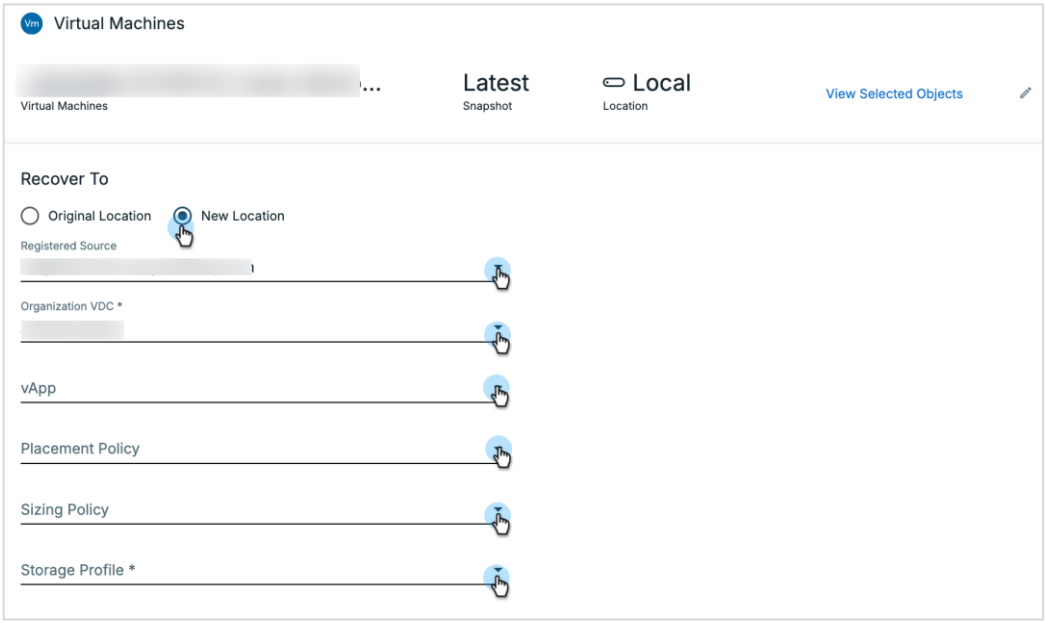
1. Log in to Cohesity and select **Data Protection** > **Recoveries**.
2. On the **Recoveries** page, click **Recover** and select **Virtual Machines** > **VMs**.



Enter a search query to match the names of the objects (VMs) you need to recover. You can use the '*' wildcard character to use partial names or to broaden your search and the filters to narrow your search. Select the VMs to recover. Under **Selected**, you can choose a different snapshot from which to recover. To continue, click **Next: Recover Options**.



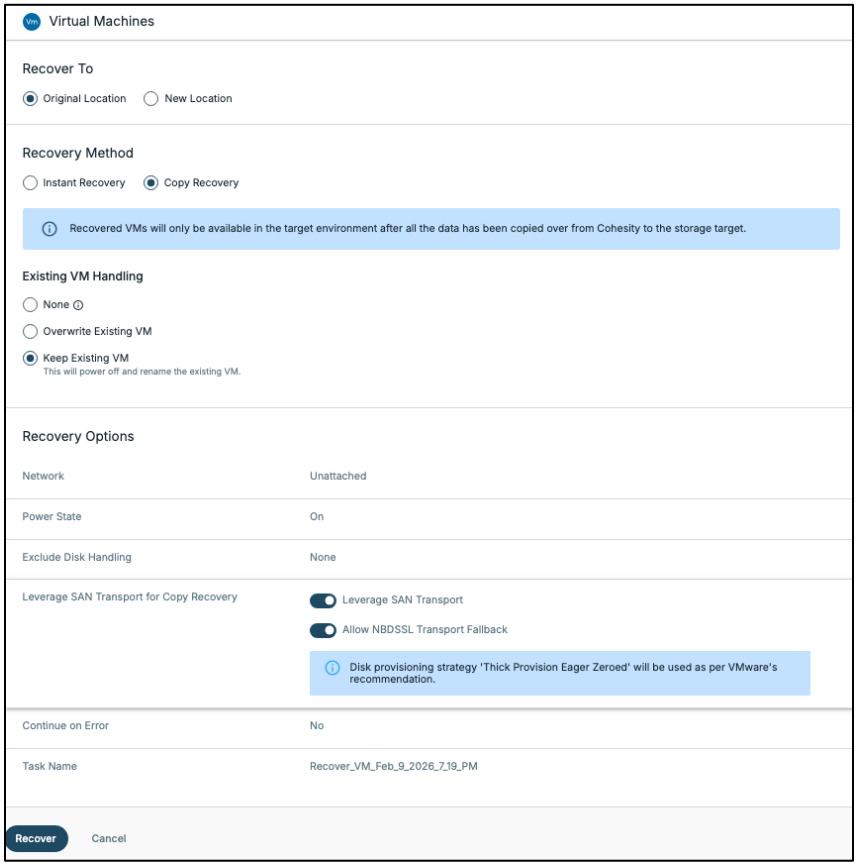
3. Select whether to recover the VMs to the **Original Location** or a **New Location**. If you select **New Location**, enter the **Registered Source**, **Organization VDC**, **vAPP**, **Placement Policy** and **Storage Profile**.



Note: Starting release 7.4, Cohesity now allows restoration of placement and sizing policies when vCD VMs are recovered to their alternate location.

4. Select the **Recovery Method** and your preference for **Existing VM Handling**:

   If you have configured the SAN transport mode for the backup, then you can leverage the SAN transport mode to recover the VM.



When the recovery task is completed successfully, the recovered VMs will be available at the selected location.

For more information on VM recovery and the Recovery Options, see Recover VMs in the online Help.
Recover vApps and vApps Templates

Cohesity provides the functionality and granularity to backup and restore vApps and vApps templates. It follows a similar workflow to recovering files and VMs. Cohesity seamless integration provides seamless backup and recovery, integrating with the self-service functionality.

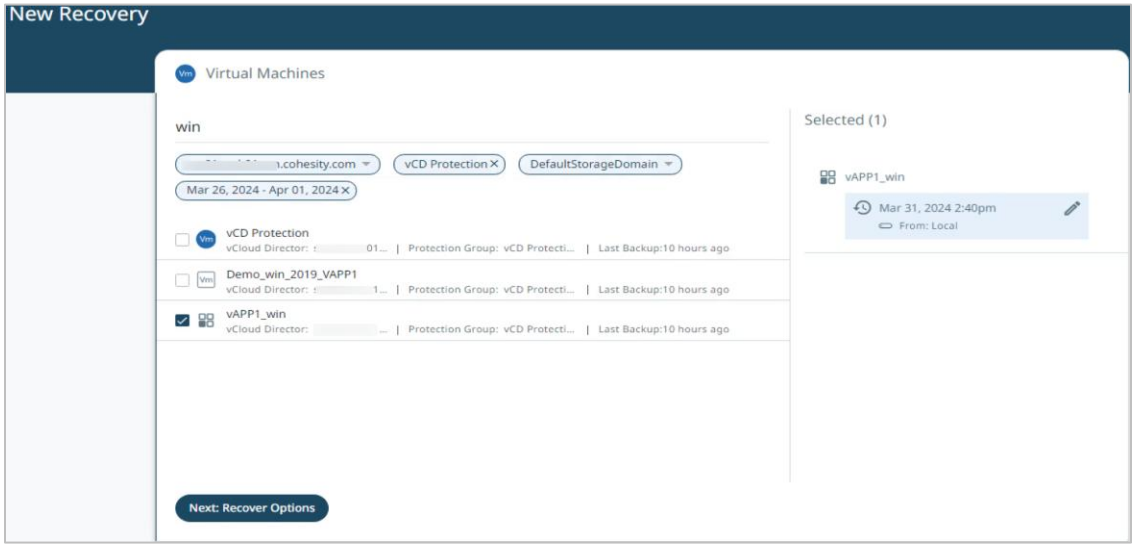
IMPORTANT: The only difference between recovering a vApp and a vApp Template is that you can only recover a vApp as a vApp, whereas you can recover a vApp Template as either a vApp or a vApp Template.

To recover a vApp or a vApp Template:

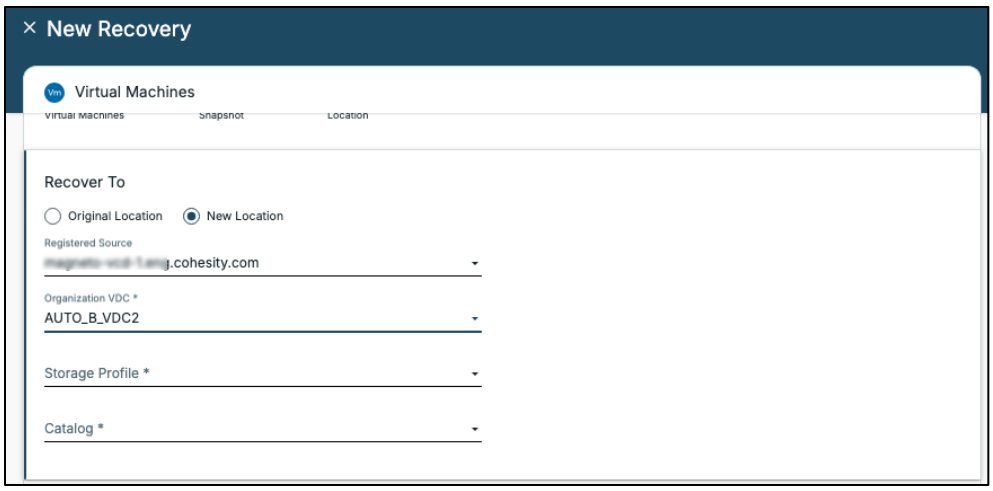
1. Log in to Cohesity and select **Data Protection** > **Recoveries**. On the **Recoveries** page, click **Recover** and select **Virtual Machines** > **VMs**.
2. Enter a search query to match the names of the objects (vApps and vApp Templates) that you need to recover. You can use the '*' wildcard character to use partial names or to broaden your search and the filters to narrow your search. Select the vApps or vApp Templates to recover. Under **Selected**, you can choose a different snapshot from which to recover. To continue, click **Next: Recover Options**.

NOTE:

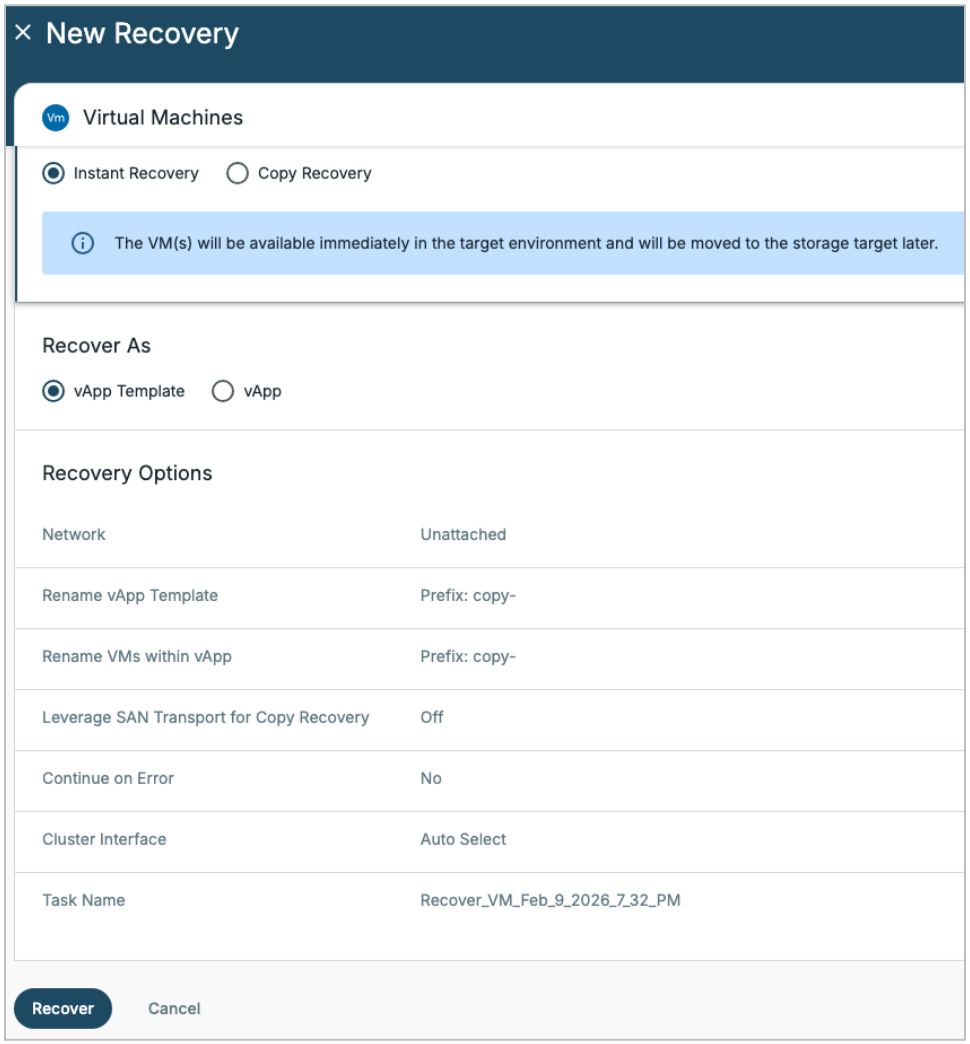
- VAPP and VAPP Template will be a selectable recovery objects in the recovery workflow only if you backed up the VAPP and VAPP Templates using Auto Protection
- You can only recover one vApps or vApp Templates in each task. You cannot select a mix of vApps and vApp Templates in the same recovery task.



3. Select whether to recover the vApps or vApp Templates to the **Original Location** or a **New Location**. If you select **New Location**, select the **Registered Source**, **Organization VDC**, **Storage Profile** and **Catalog**.



4. Select the **Recovery Method** and your preference for **Recovery Options**:



5. Configure the other Recovery Options and click **Recover**. This creates a recovery task.

When the recovery task is completed successfully, the recovered vApp or vApp Template will be available.

For more information on vApp and vApp Template recovery and the Recovery Options, see Recover VMs in the online Help.

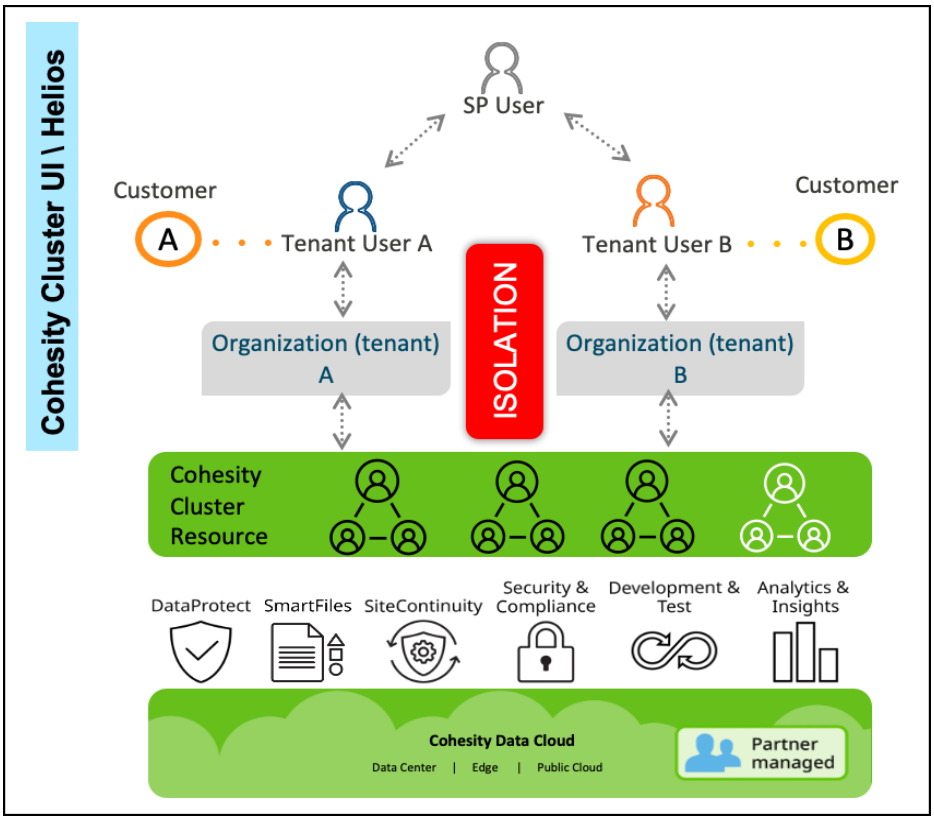
Enable Multi-Tenancy on Cohesity

Multitenant solutions provide great flexibility and logical isolation by leveraging the same hardware platform, which multiple customers can use without interfering with each other's data sources. However, multitenant solutions come with the enormous challenge of manageability, and the applications that support them will also comply with the same rule of isolation and adhere to the multitenant solution.

VCD is a multitenant solution from VMware that allows multiple customers to leverage the same underlying hardware. The data protection solution will also adhere to the multitenant architecture and provide ease of manageability with isolation between the organizations. Cohesity delivers simplicity with the multitenancy of VCD and supports two different architectures for service providers; either a service provider can manage the organization, or a customer will leverage the self-service backup and restore via the VCD plugin.

Before starting with the Cohesity multitenancy, let's understand the isolation between the customer with the following diagram.

Figure 4: The Isolation Between Customers



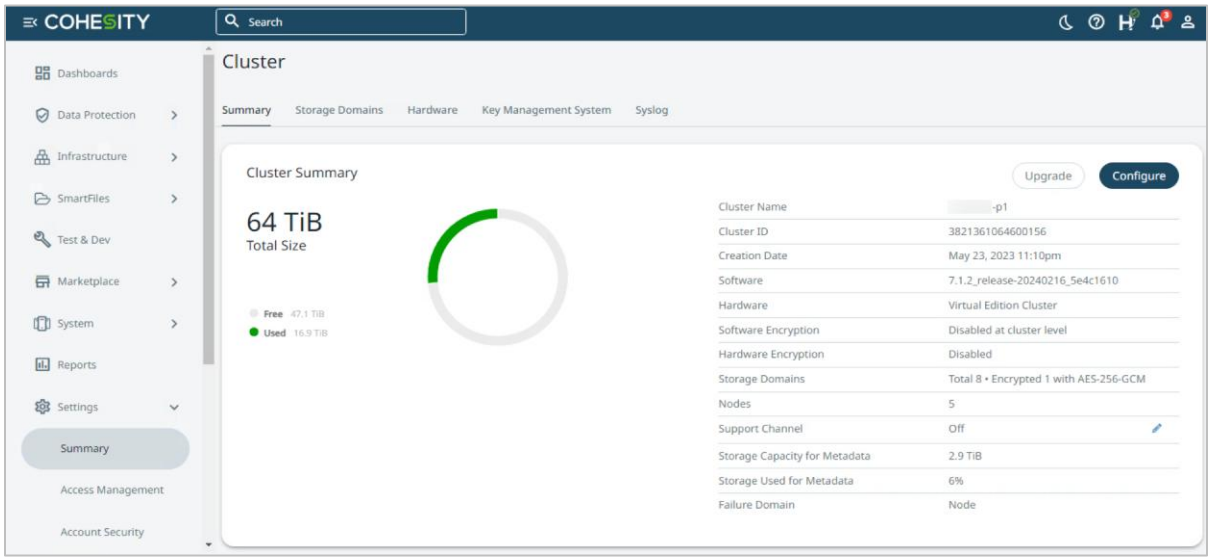
Configuring multi-tenancy on Cohesity is intuitive but requires some initial setup. Once you complete these steps, you can map VCD Organizations to Cohesity Organizations.

To start using multi-tenancy on Cohesity, the first step is to enable Organizations in the Cohesity cluster.

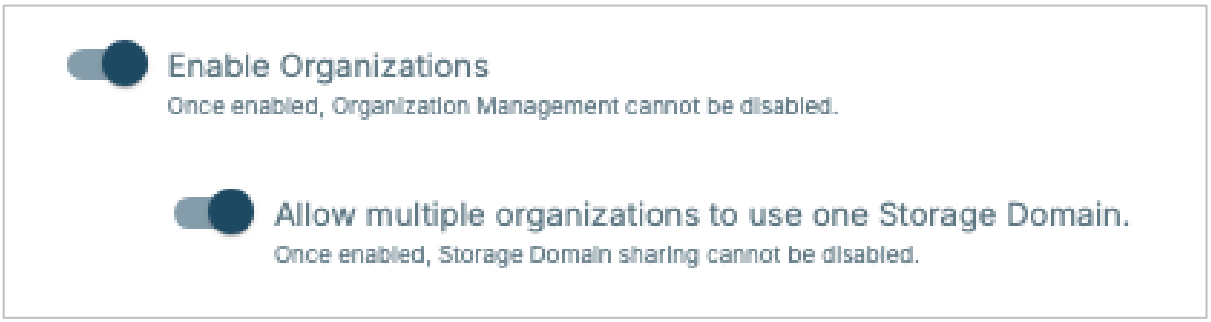
NOTE: You cannot disable the Organizations functionality on that Cohesity cluster once you enable it.

To enable Cohesity Organizations:

1. Log in to Cohesity, navigate to **Settings** > **Summary**, and click **Configure**.



   On the **Edit Cluster Settings** page, click **Enable Organizations**. You can also enable the **Allow multiple organizations to use one Storage Domain** option, but if you do, you cannot subsequently disable Storage Domain sharing.



2. Scroll down to the bottom of the page and click **Save**.

Multi-tenancy is now enabled on your Cohesity cluster.

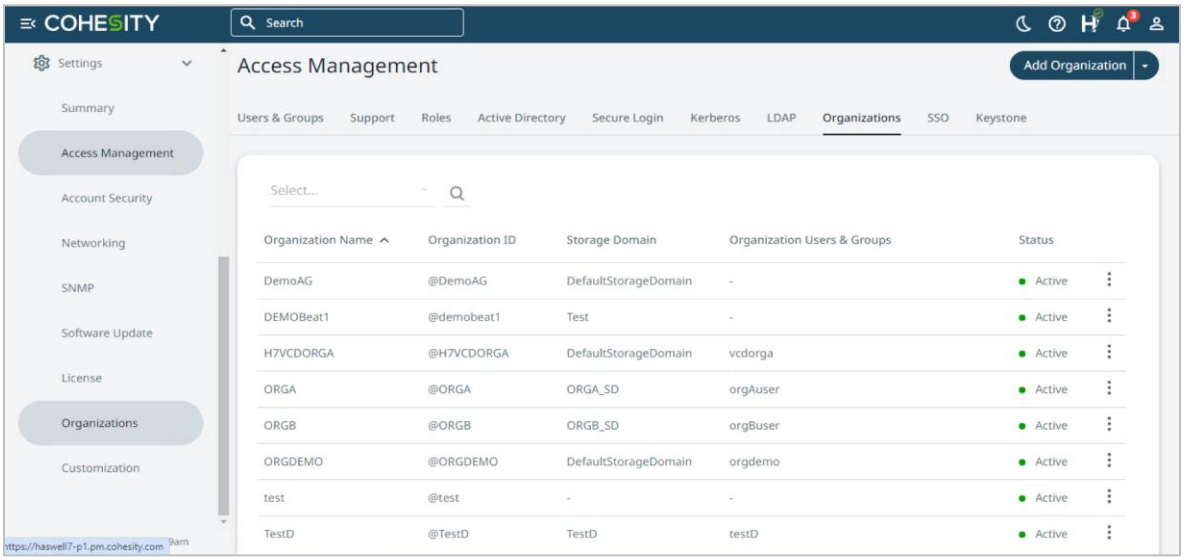
Service Provider: Create Cohesity Organizations and Map to VCD Organizations

Once multi-tenancy is enabled on the Cohesity cluster and VCD is registered as a Cohesity source, the next step is to map the Organizations on Cohesity with VCD Organizations.

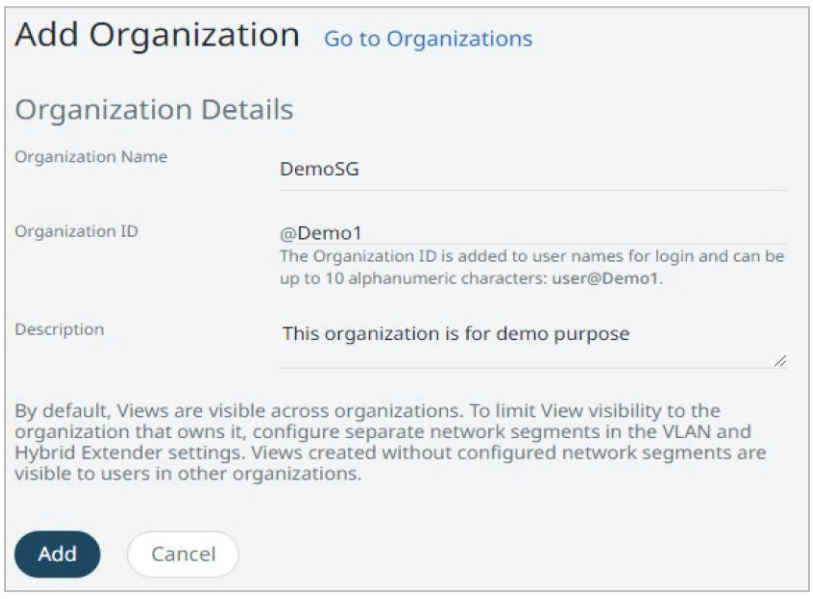
NOTE: Before you proceed, ensure there are Organizations on your VCD to which you can map your Cohesity Organizations.

To create a Cohesity Organization:

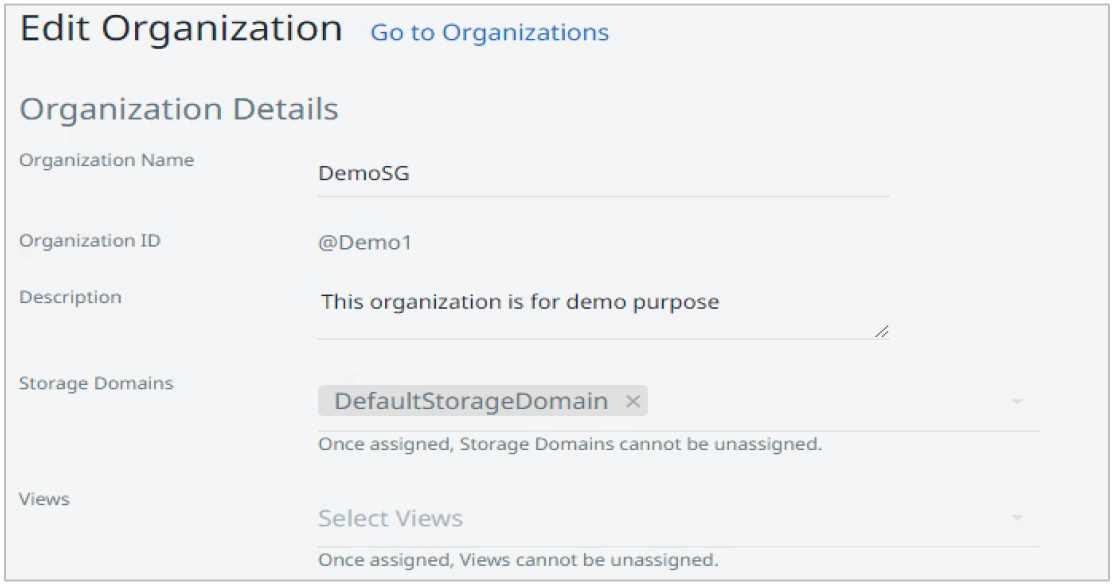
1. Navigate to **Settings** > **Organizations**, click the **Organizations** tab, then click **Add Organization**.



2. On the **Add Organization** page, enter the **Organization Name** and **Organization ID**, add a **Description**, and then click **Add**.



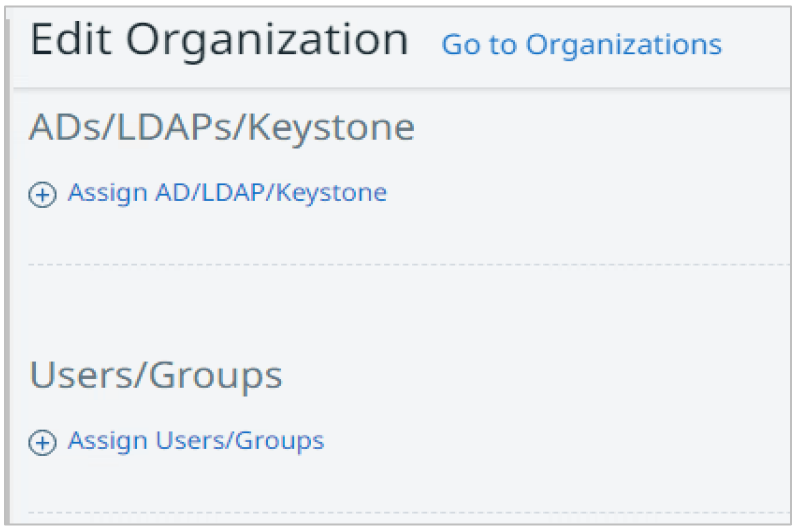
3. On the **Edit Organization** page, select the **Storage Domains** that you want to assign to this Organization.



NOTE: If necessary, you can also **Add Storage Domain** directly from this drop-down and assign it to this Organization. You can assign more **Storage Domains** after you've created the Cohesity Organization.

4. Under **ADs/LDAPs/Keystone**, click **Assign AD/LDAP/Keystone** to add an existing or new authentication source.

5. Under **Users/Groups**, click **Assign Users/Groups**. You can assign existing users and groups, or you can create new users and groups. You can also assign users and groups after you've created the Organization. Cohesity supports SSO users and groups for Multitenancy.



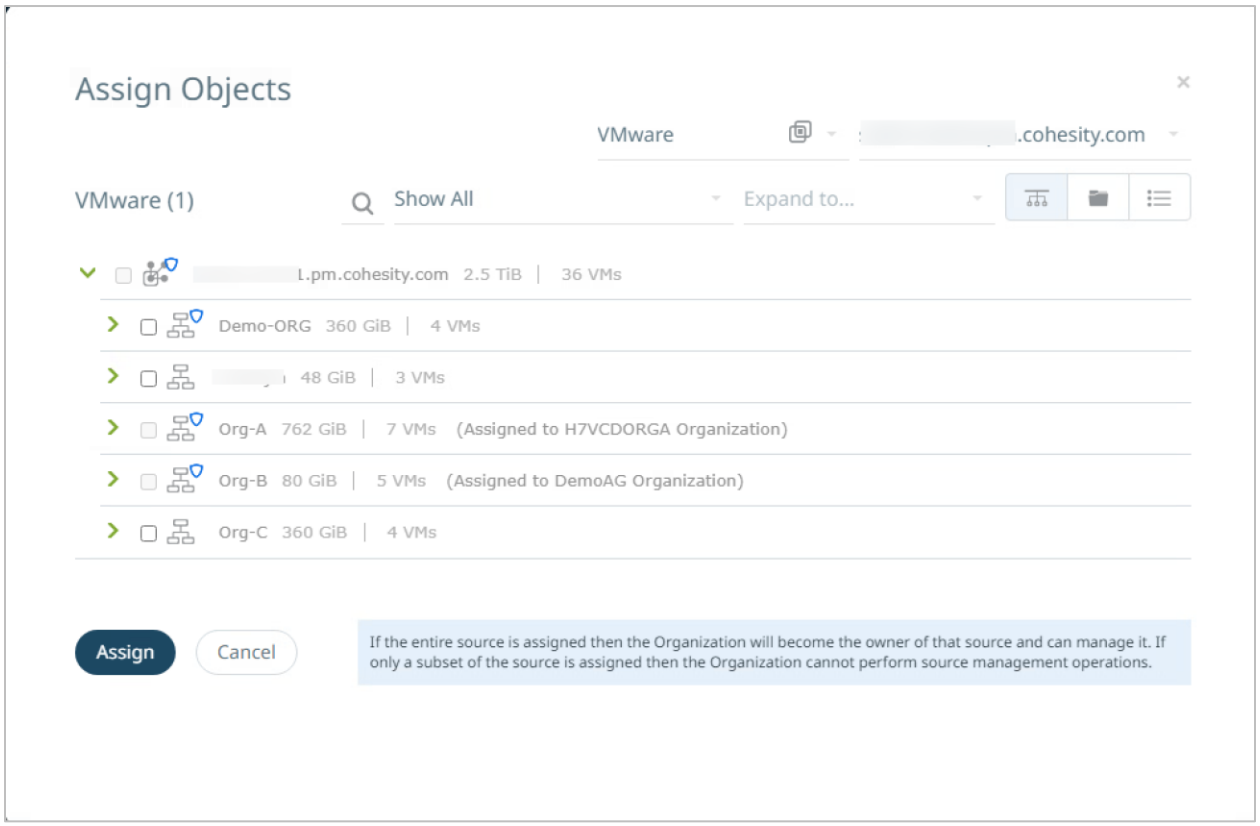
Now that you have your Cohesity Organization, the next step is to map it to a VCD Organization in the next Sources section within this same **Edit Organization** page.

Map VCD Organizations to Cohesity Organizations

To map a VCD Organization to this Cohesity Organization:

1. On the **Edit Organization** page, under **Sources**, click **Assign Objects**.

   In the **Assign Objects** form, Select the VMware and **VCD IP/FQDN** you used to register your VCD source. Expand the VCD, select the VCD Organization you want to map to this Cohesity Organization, and click **Assign**. All the existing resources (including those created in the future) under the selected VCD Organization will be available for management by this Cohesity Organization. Once you have been assigned the VCD organization, you cannot assign it to another Cohesity Organization. Mapping the organization is a 1:1 mapping.

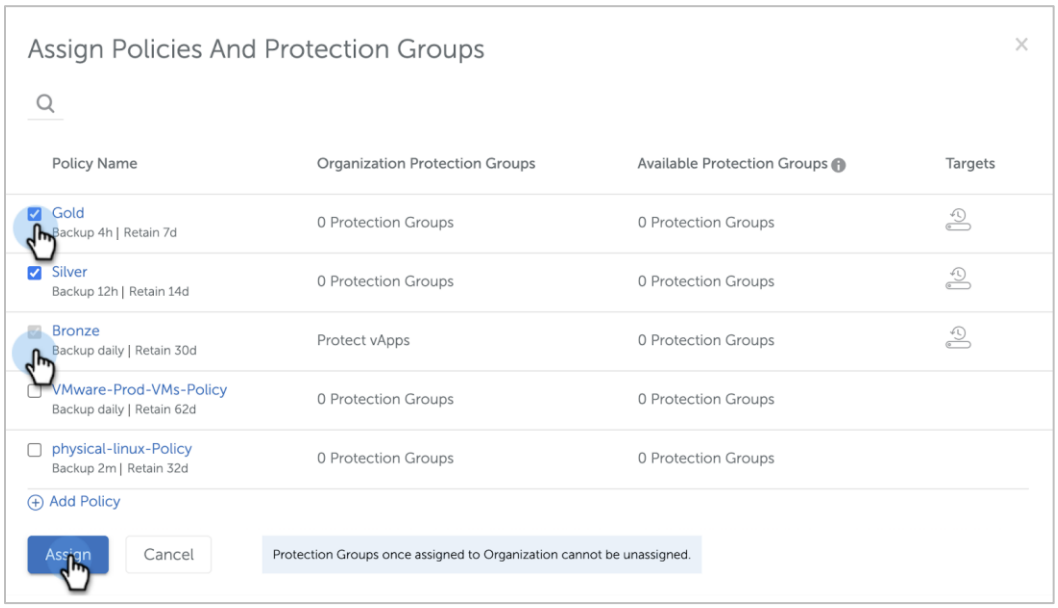


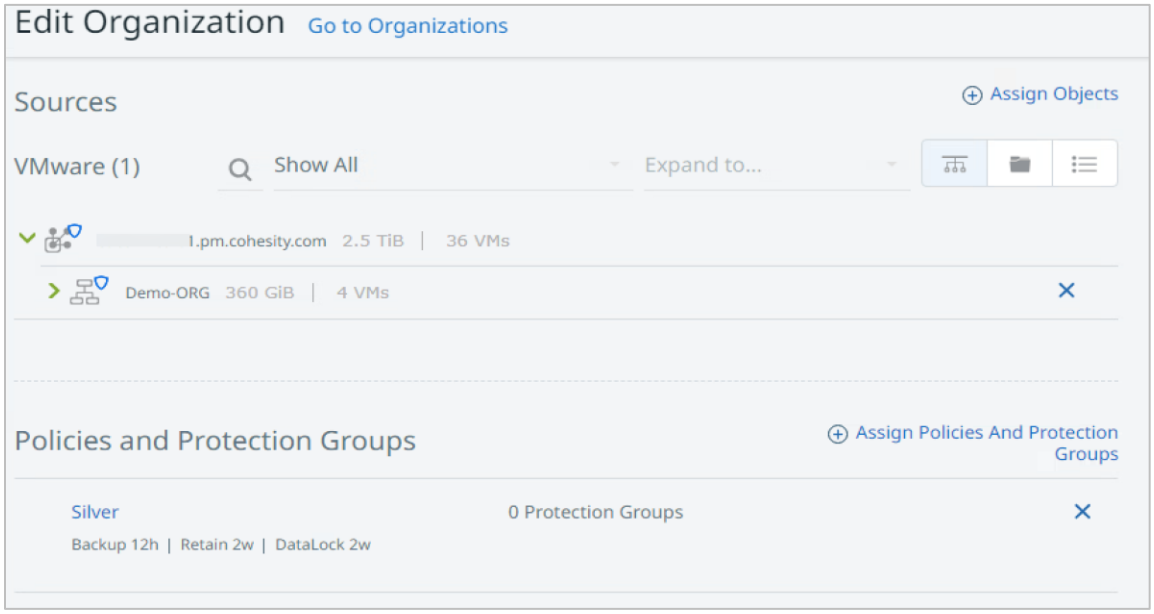
2. Under **Policies and Protection Groups**, click **Assign Policies and Protection Groups** to select the Protection Policies you want to use.

   NOTE: Protection Groups that are protecting any assigned sources in the same Storage Domain are automatically assigned to this Organization.

3. Select the Protection Policies that you want to make available to this Organization and click **Assign**.

NOTE: Once you assign a Protection Group to an Organization, you cannot unassign it.





Now that you have mapped your organizations, you'll need to configure the networking requirements to provide network isolation for tenants within this same **Edit Organization** page.

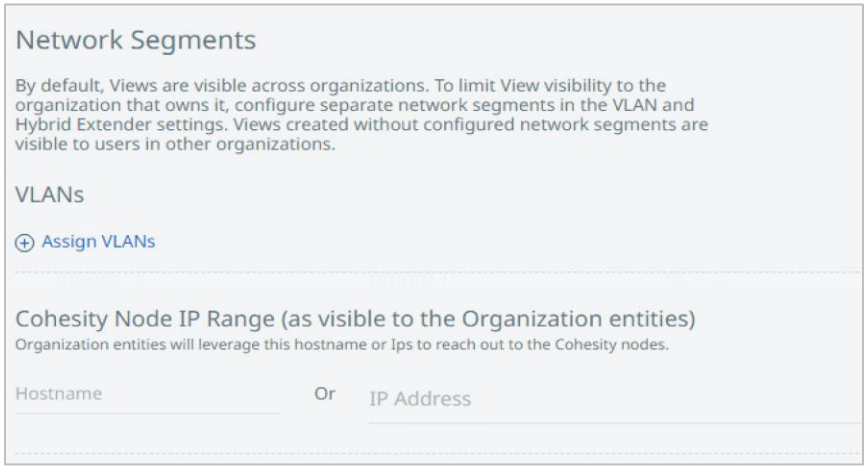
Configure Networking Requirements on Cohesity

The next step is to configure the network for the organization. Cohesity recommends having a dedicated VLAN for the organization to be aligned with the underlined concept of isolation. You can configure the VLAN on the Cohesity cluster and assign it to the organization, or you can create a new VLAN while configuring the organization.

NOTE: For details, see Configure Network Settings for an Organization in the online Help.

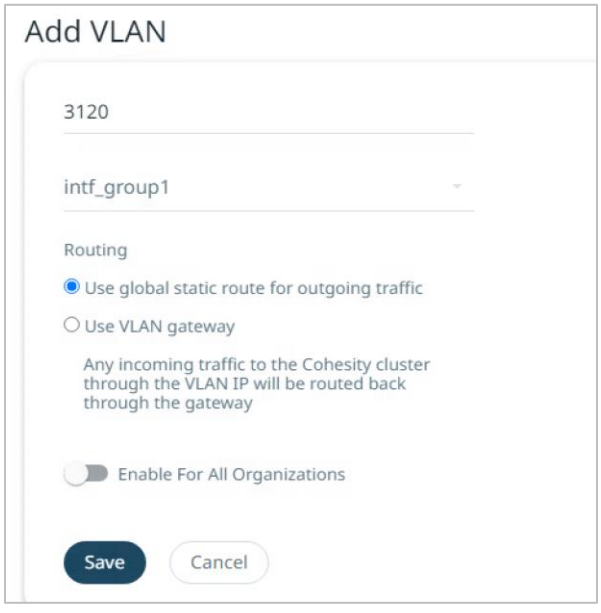
To set up networking:

1. Under **Edit Organization > Network Segments** > **VLANs**, click **Assign VLANs**.

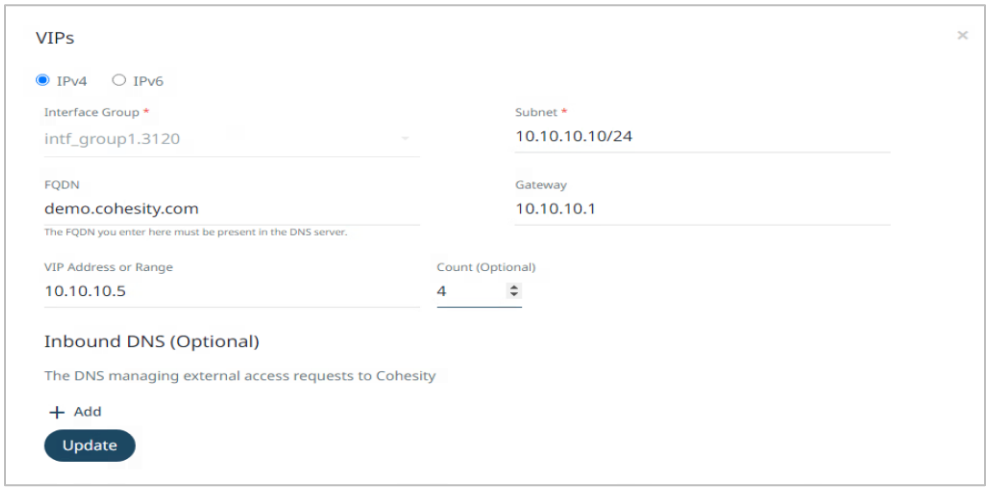


2. Click **Add VLAN.**
3. Select the **Interface Group**, enter the **VLAN ID** you want to assign, and select the IP addressing scheme (IPv4 or IPv6).

NOTE: You can also enable this VLAN for all organizations.



4. Click on **Add VIP** and enter **Subnet**, **Gateway**, **FQDN**, and **Gateway** details.

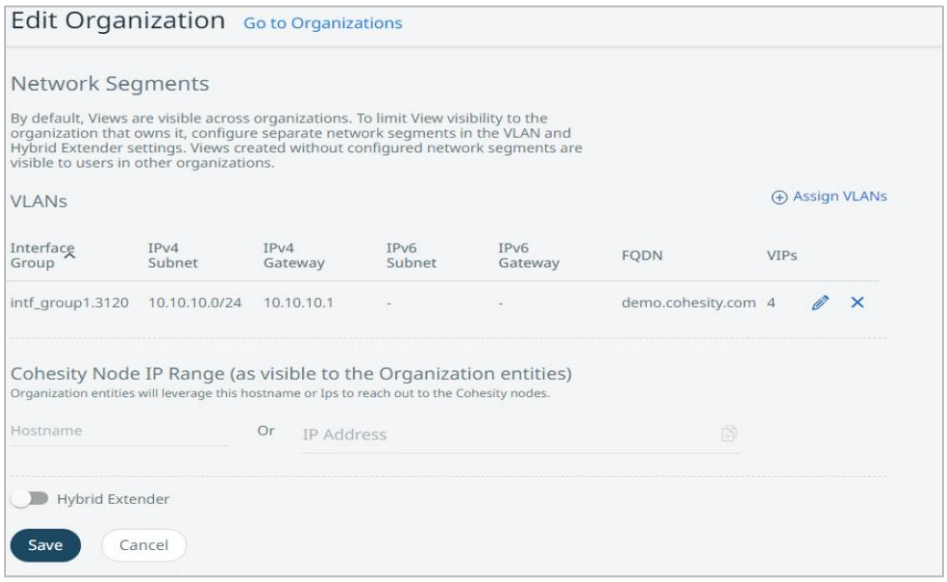


You can also assign a Cohesity Node IP Range that's visible to Cohesity Organization entities, which these entities will use to reach out to Cohesity nodes. For more details about network configuration for VCD, see *Isolate Tenant Networks Using VLANs* in the Backup as a Service Technical Solution Guide.

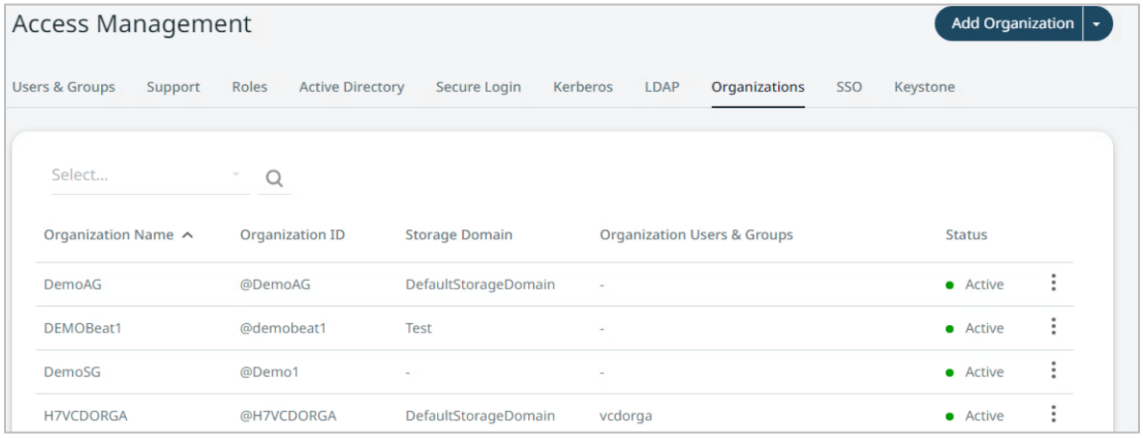
Alternatively, you can use Cohesity's Hybrid Extender to overcome IP address conflicts across the tenants. See Hybrid Extender in the online Help.

5. Click **Assign to** assign the VLAN that you just created to this Organization.

6. Click **Save** to save all the settings and create this Organization.



Your new Cohesity Organization appears on the **Organizations** tab under **Settings > Access Management**.



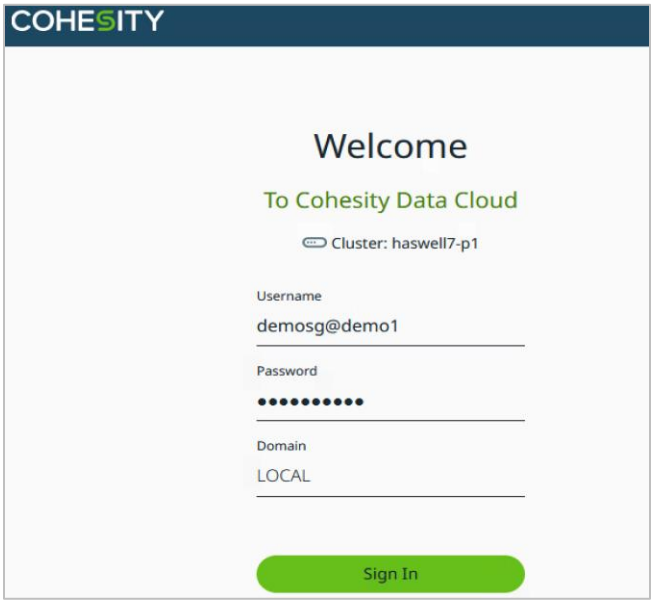
VCD Organization User: Protect VCD Resources on Cohesity

Once the service provider (SP) has created a Cohesity Organization and mapped it to a VCD Organization, the VCD Organization user can log in using the Cohesity Organization user account that the SP assigned earlier and immediately start protecting their VCD Organization's data on Cohesity.

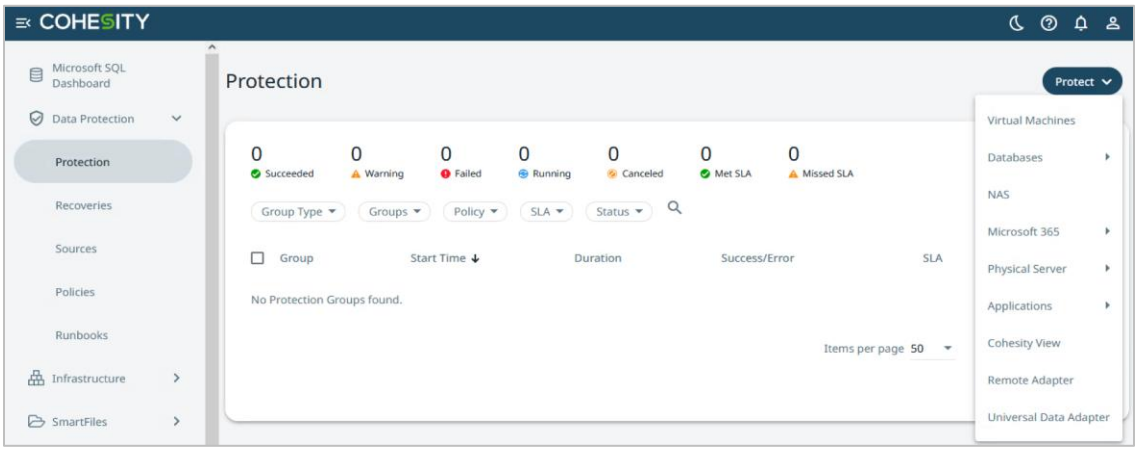
NOTE: This workflow is performed as a tenant as part of self-service either from the Cohesity cluster or Helios.

To protect the assigned VCD Organization on Cohesity:

1. Log in to Cohesity using the Cohesity Organization user credentials.

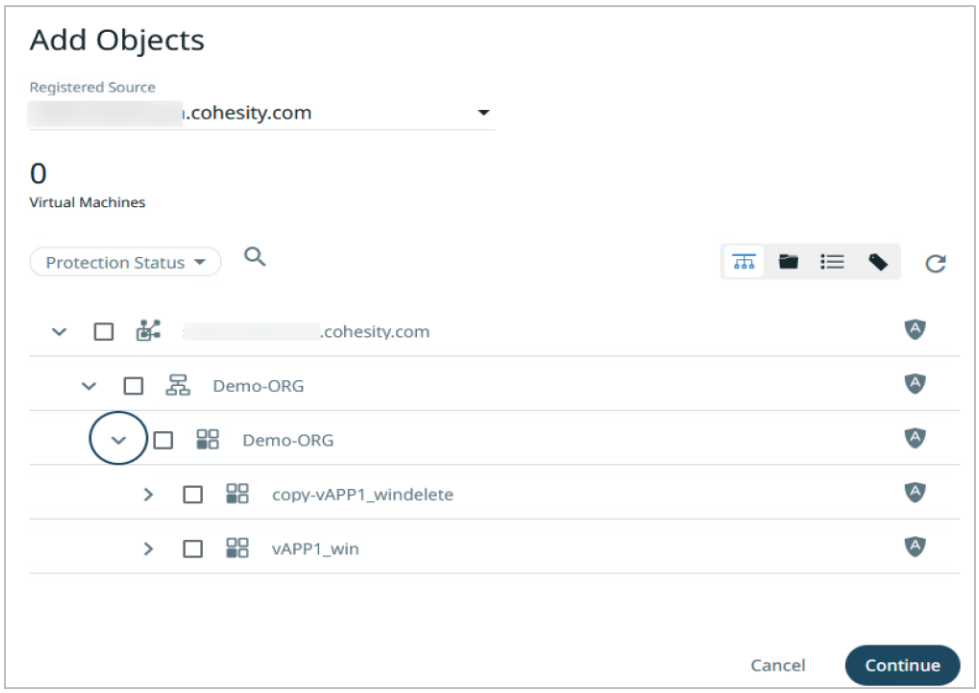


2. Once you log in, you are redirected to the **Protection** page, where you can click **Protect** and select **Virtual Machines** to start protecting the VCD Organization and their objects mapped by the service provider to this Cohesity Organization in the previous steps.



3. In the **New Protection** page, select the **vCloud Director** source under Sources.

NOTE: The Cohesity Organization user who is logged in will only see the VCD Organizations that were assigned to this Cohesity Organization, which the service provider maps to intact with the concept of isolation.



To finish setting up this protection, follow the steps for protecting Organizations, vApps, VMs, and more.

You can add other sources for protection, such as physical servers, as a tenant (Cohesity Organization) and protect them separately from the assigned VCD resources. For details, see Supported Multitenancy Workflows in the online Help.

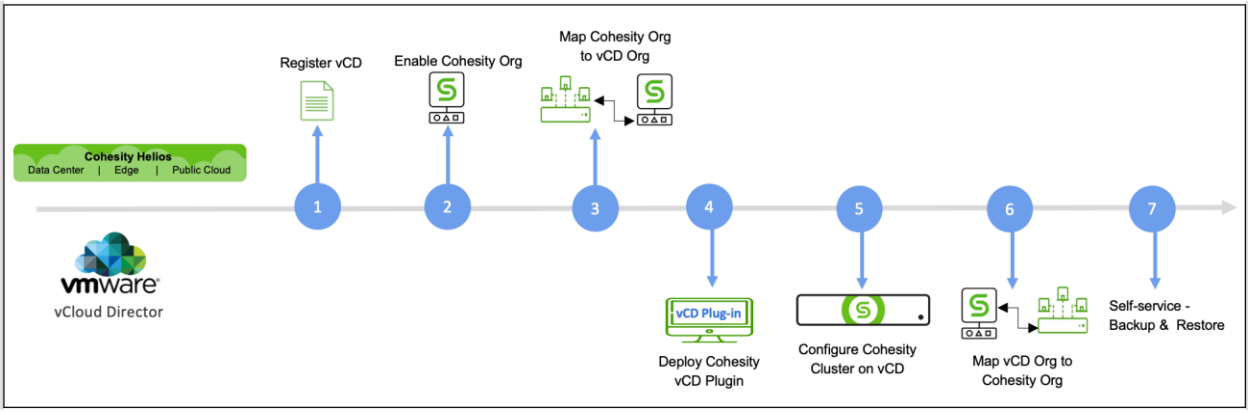
To recover protected VCD sources for this Cohesity Organization, follow the steps in Recover VMware Cloud Director Objects above.

Use Cohesity VCD Plugin for VCD Tenant Self-Service

To make our customers' experience seamless by providing a single interface for managing all your backup, recovery, and other Infrastructure-as-a-Service (IaaS) tasks, we provide a VCD extension to deliver cloud services (IaaS in this case) with self-service on top of your existing VMware infrastructure. This extension integrates natively with the VMware Cloud Director UI for tenant self-service. Customers can manage the infrastructure assigned to them from the VCD UI, and there is no need to log in or perform any operation from the Cohesity cluster UI.

Self-service is delivered securely through role-based access control. The following workflows are supported using Cohesity's extension for VCD:

- Protection status dashboard
- Protect and unprotect VMs, vApps, and vApp templates
- Restore VMs, vApps, and vApp templates
- Restore files and folders
- Monitor backup and restore tasks
- Cross-launch to Cohesity UI for advanced services



To set up the Cohesity VCD extension for tenant self-service:

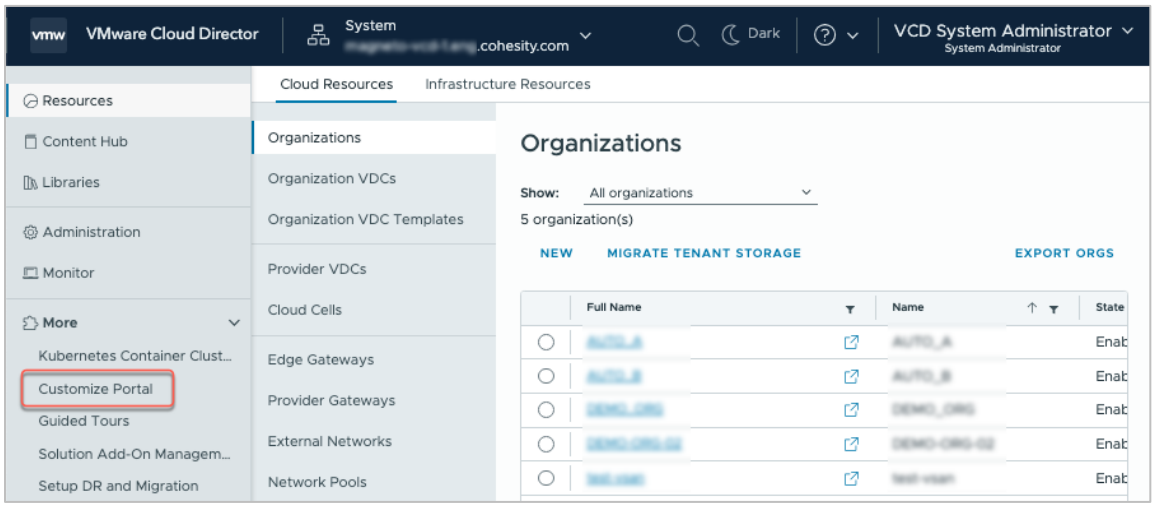
1. Install the VCD extension. (*Service provider*)
2. Configure VCD and map Cohesity Organizations to your VCD Organizations. (*Service provider*)
3. Perform the steps in the tenant VCD data protection workflow. (*Service provider & tenants*)

Install VCD Extension

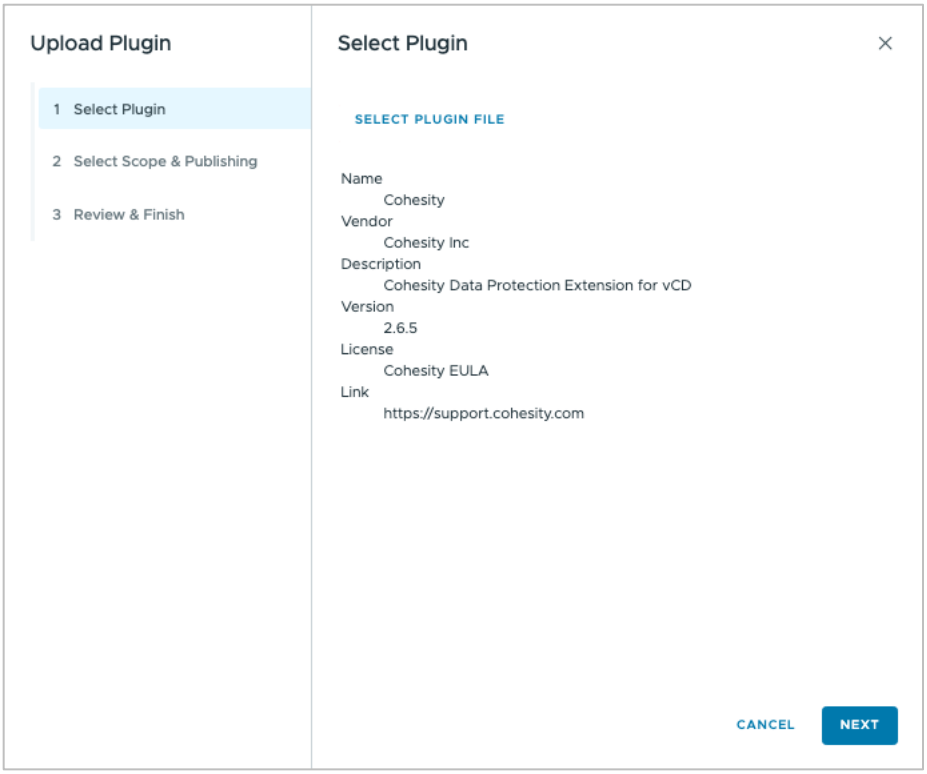
Before installing the VCD plugin, make sure certain prerequisites are met. This will help you have seamless experience with Cohesity's VCD extension. The VCD extension code and documentation are publicly available on our VCD extension GitHub page. Follow the installation instructions there to install the extension. The service provider must install the VCD plugin.

Installation of the VCD plugin is an easy and three-step process:

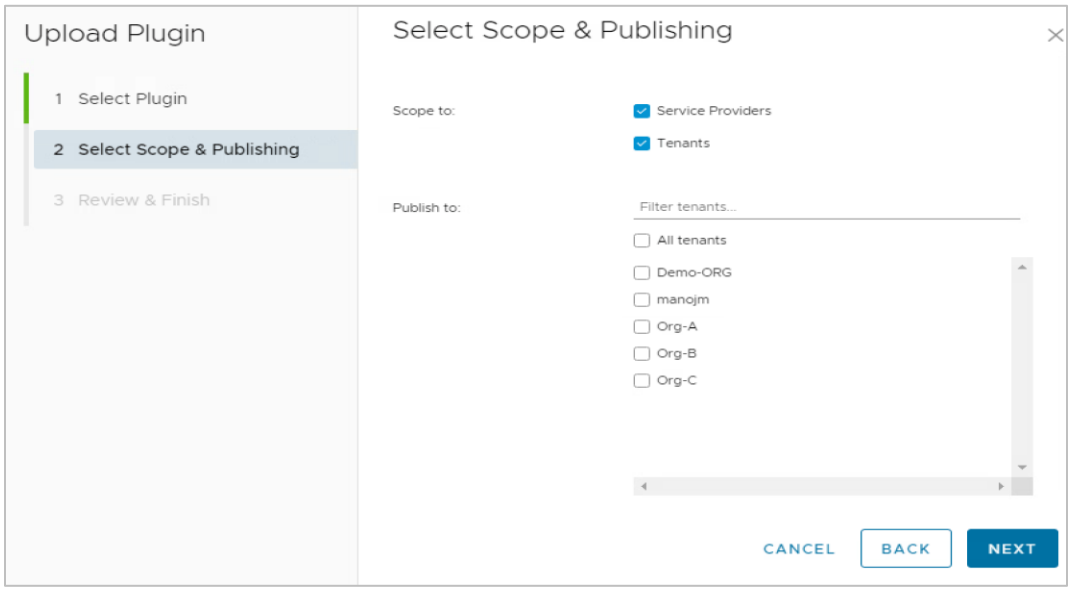
1. Download the VCD plugin from GitHub.
2. Navigate to the **More > Customize Portal.**



3. On the plug-in page, click **upload**.
4. Select the downloaded plugin file and click **Next**.



5. The next page will ask you to set the scope, which means you will put the scope and publish the plugin for the specific organization. Cohesity provides flexibility to choose the self-service option according to the service provider's needs.



6. Click **Finish**. This will install the plugin with the VCD, which you can use after refreshing the browser.

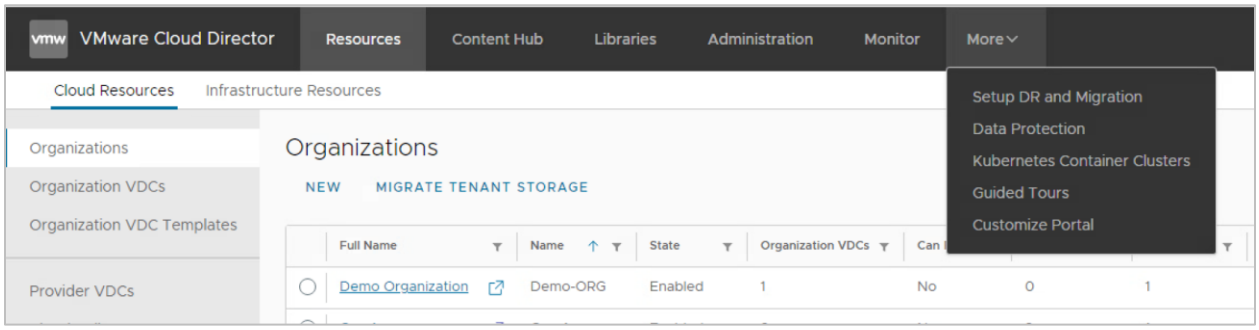
Configure VCD and Map Cohesity Organizations to VCD Organizations

Once the Cohesity extension is successfully deployed in VCD, you need to configure the Cohesity cluster in VCD and map the Organizations (tenant) you created on your Cohesity cluster to your VCD Organizations.

To configure VCD and map Organizations:

1. Log in to the VCD as a service provider with admin credentials.

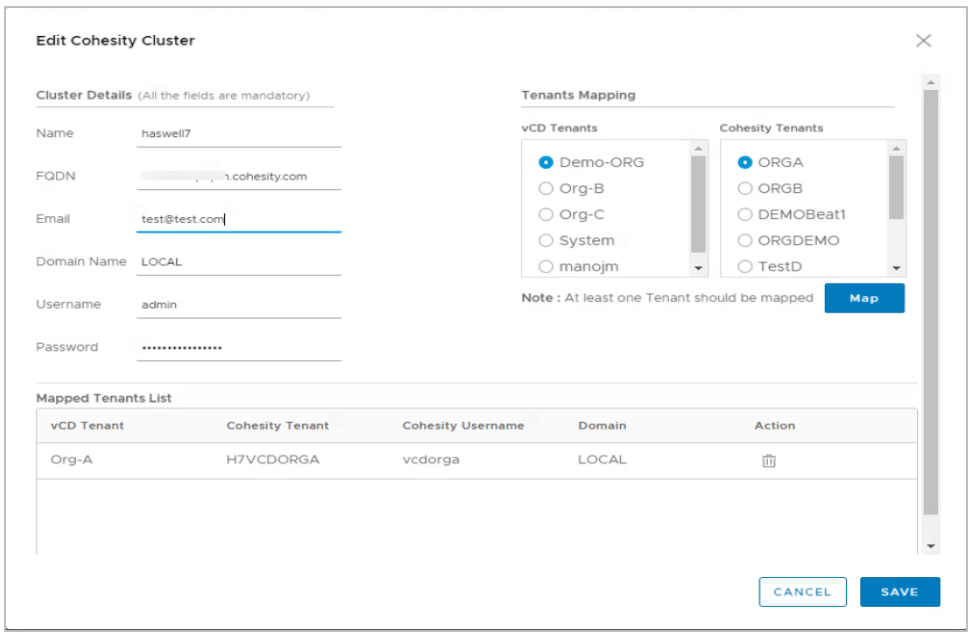
2. Post installation of the VCD plugin, you can see the new option in the **Data Protection** menu bar.



3. Click **Add** and provide the cluster details. You can see all the organizations configured in the Cohesity cluster.

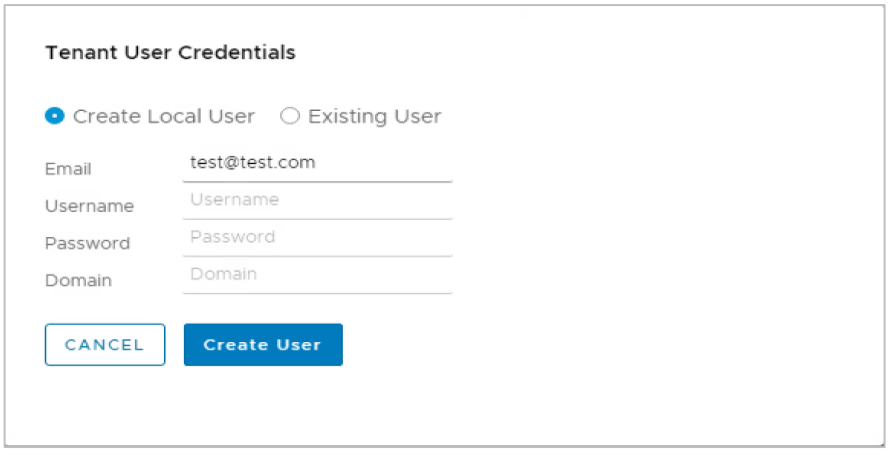
4. In the **Edit Cohesity Cluster** page, enter the Cohesity cluster details, such as the cluster's IP address or hostname and SP user credentials. The Cohesity Organization is listed in the **Tenants Mapping** section.

   Select the **VCD Tenants** and the **Cohesity Tenants** and click **Map**. This will assign the selected Cohesity Organization to the selected VCD Organization. In the background, the extension will give the right access to the VCD Organization to protect their VCD resources on Cohesity under the Cohesity Organization assigned to it. This mapping also provides the needed isolation among VCD Organizations, as they can now log in to the assigned Cohesity Organization and protect their VCD resources without any visibility to other Cohesity and VCD Organizations, thus achieving multi-tenancy.



5. In the **Tenant User Credentials** form, you can either **Create New Local User** (the user is created automatically) or select an **Existing User** (Local or Active Directory user), which are already configured with the Cohesity organization.

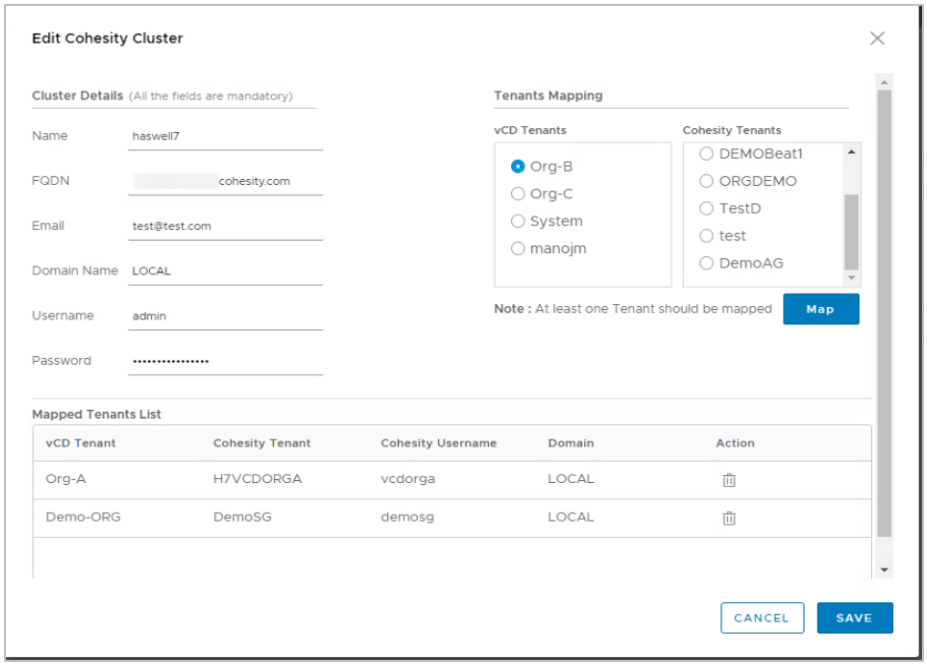
   For existing users, you need to provide only the username without any organization name.



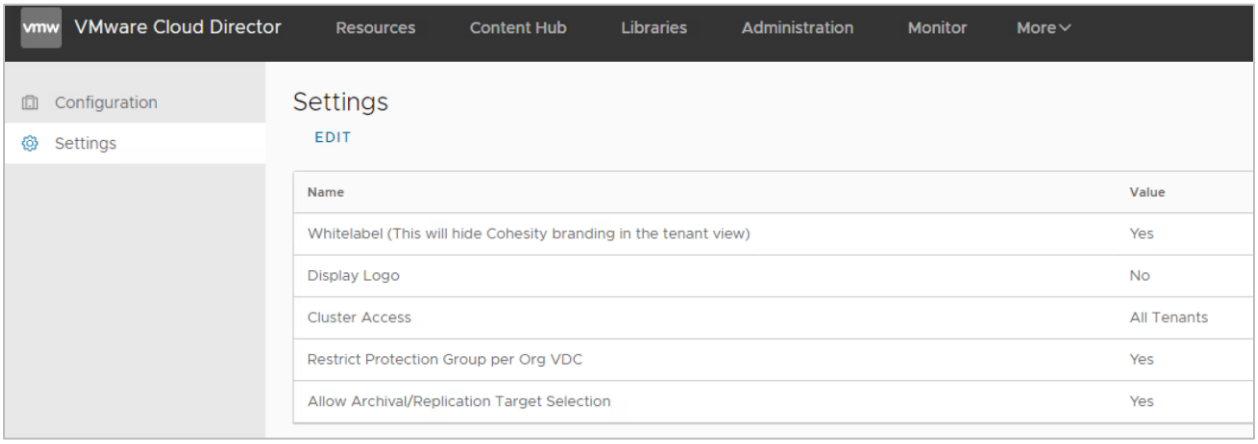
NOTE: SSO (Single Sign-On) users are not supported.

   These organizational user credentials are used to make API calls to the Cohesity cluster to run all workflows for the tenant. To run the workflows, the tenant user must hold the Cohesity privileges. For more details, refer to Access Management: Privileges for Service Providers and Tenants.

6. Click **Save**. The mapping is now created and the Cohesity cluster is added. The VCD Organization user can now access Cohesity workflows through his tenant portal.



7. You can edit several additional multi-tenant features for each VCD Organization that is now mapped to a Cohesity Organization. Go to **Settings** and click **Edit** to configure:
   - **Whitelabel**. Hide Cohesity branding from your tenant.
   - **Display Logo**. Choose to show or hide the Cohesity logo in the VCD extension.
   - **Cluster Access**. Specify which VCD Organizations can cross-launch to their Organizations on their Cohesity cluster.
   - **Restrict Protection Group per Org VDC**. A single Protection Group cannot protect objects across different Organization vDCs.
   - **Allow Archival/Replication Target Selection**. This option allows users to select the archival and replication targets during an on-demand backup.



Perform Tenant VCD Protection Workflow

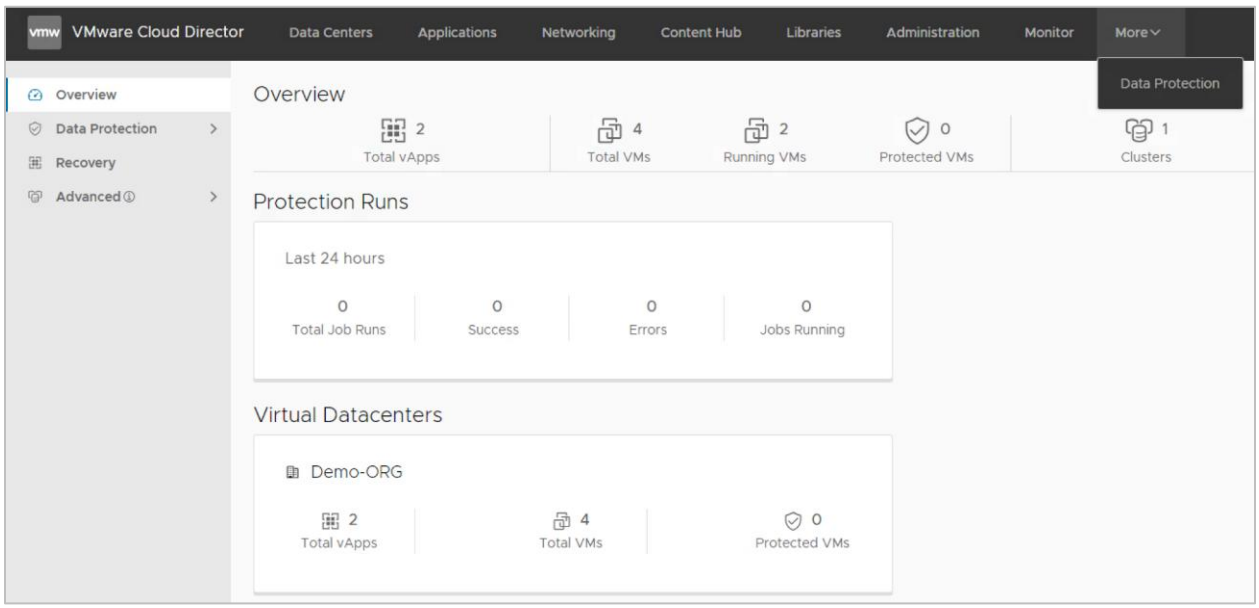
The Cohesity VCD plugin supports all the major workflows, and we are constantly working on adding new workflows to it. In this solution guide, we have covered all the supported workflows. The VCD plugin provides a dashboard for VCD that summarizes all the information on one page. The dashboard will give an idea of the data protection of the VCD organization.

The top section of the dashboard provides an overview of the VCD Organization and shows the number of Virtual Datacenters (vDCs), Running vApps, Running VMs, and resources used.

The **Virtual Datacenters** section lists all the vDCs in the VCD Organization, along with their individual resource utilization. It also shows the number of vApps in each vDC and the number of VMs running in these vDCs.

You can view the dashboard after the plugin installation by clicking on the new Data Protection bar in the menu.

Figure 5: VCD Organization Resource Utilization Overview



To protect your VCD data as a tenant, log in to VCD UI using your tenant credentials and:

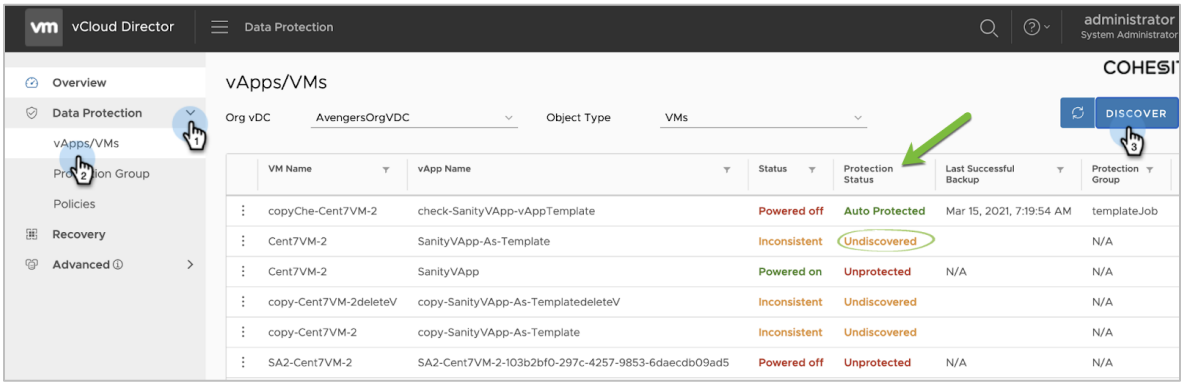
1. Discover the VMs and vApps in your VCD environment.
2. Protect your VMs, vApp, and vApp Templates.
3. Restore your VMs and vApps.
4. Restore or download files and folders.
5. Cross-launch the Cohesity UI from the VCD extension.

Discover VMs and vApps

The first step is to ensure that Cohesity discovers your VMs. You can check the status based on the **Protection Status** field.

To discover the VMs and vApps:

1. Log in to the VMware vCloud Director as the tenant, click the menu in the title bar, and select **Data Protection**.
2. On the left, expand **Data Protection** and click **vApps/VMs**. Check the status of all the VMs in the **Protection Status** field. If the status is Undiscovered for any VM, click **Discover**.



This initiates a refresh of the VCD source hierarchy registered on the Cohesity cluster. The **Refresh** icon next to the **Discover** button refreshes the page without reloading the entire page.

The Protection Status field can have one of the following values:

- **Auto Protected**. The parent node is protected.
- **Protected**. The node is protected on its own by a Cohesity Protection Group.
- **Unprotected**. The node is not protected or is excluded from Auto Protection.
- **Undiscovered**. The node is not discovered in the protection source list in the Cohesity REST API response.

Protect VMs, vApps, and vApp Templates

There are two workflows for protecting your VMs, vApps, and vApp Templates as a tenant:

- Protect individual VMs, vApps, and vApp Templates.
- Protect multiple objects in the same VCD Protection Group.

Protect Individual VMs, vApps, and vApp Templates

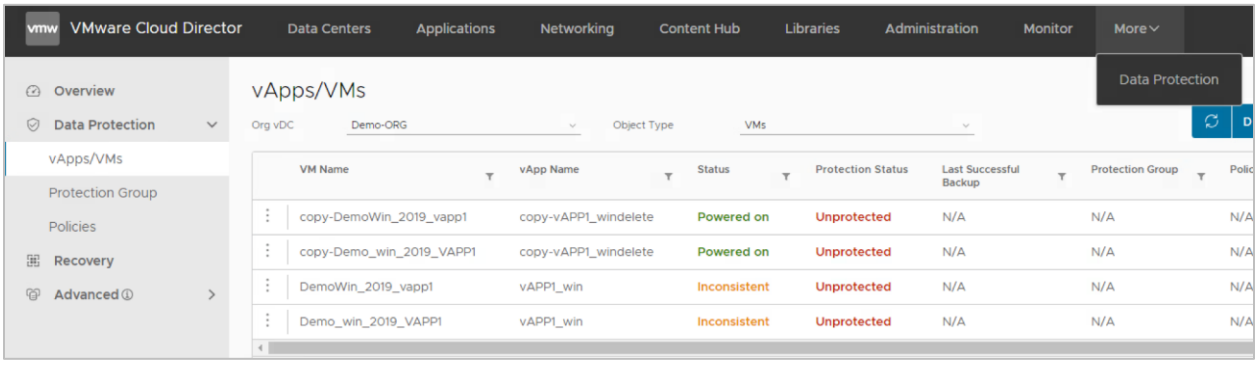
To protect a specific VCD object, you must create a Protection Group following the process below.

NOTE:

- By following the method below, you can only protect a single object. To protect multiple objects, refer to the section.
- The state of the VCD object must be discovered and not inconsistent. See Discover VMs for details.
- Any object can only be protected by one VCD Protection Group in VCD in this workflow. Once protected, the only option you have is to change it to **Unprotected** or **Backup** the object for this workflow.

To protect individual VMs, vApps, and vApp templates:

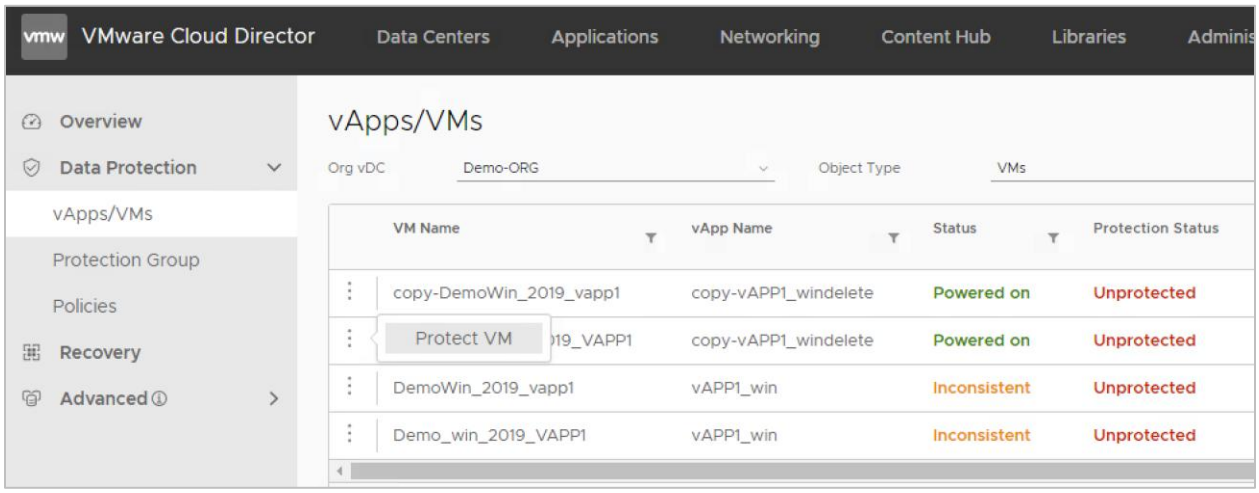
1. Log in to VCD as the tenant user.
2. Click the menu in the title bar and select **Data Protection**.
3. In the **Data Protection** menu, click **vApps/VMs.**



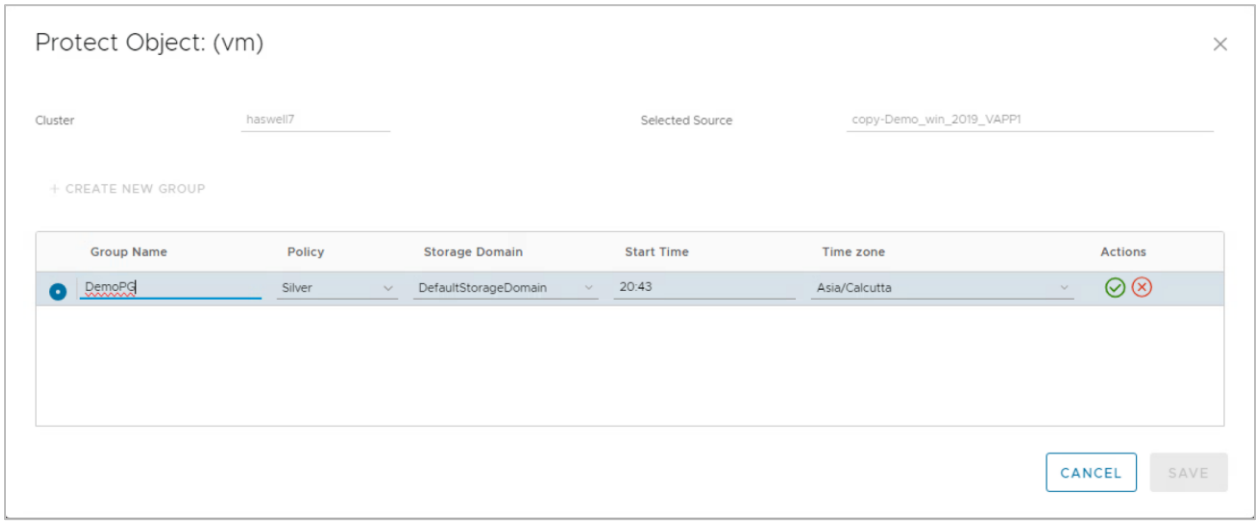
4. You can also use the **Org vDC** and **Object Type** filter on the top to list and filter the objects based on the selected vDC or choose from the listed VMs, vApps, and vApp Templates.

   Verify the status of the object in the **Protection Status** column. If any of the objects that you want to back up are in an **Undiscovered** state, then you must first discover that object. See Discover VMs.

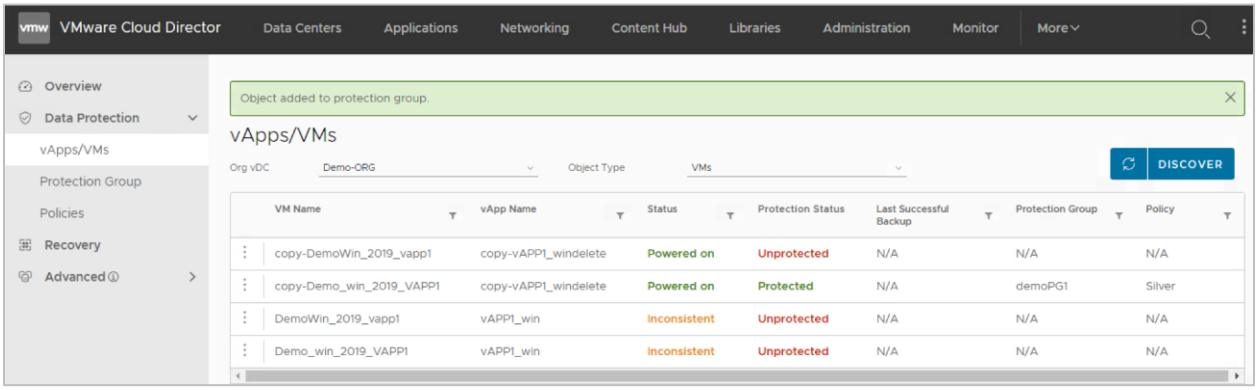
   Once the object's status changes to **Unprotected**, click on the ellipsis (⋮) on the row for the unprotected object and select **Protect VM** (or **vApp** or **vApp Template**). If you choose **AutoProtect Object** (for a vApp or vApp Template), any VM that belongs to that object or any new VM created in that object will be protected automatically.



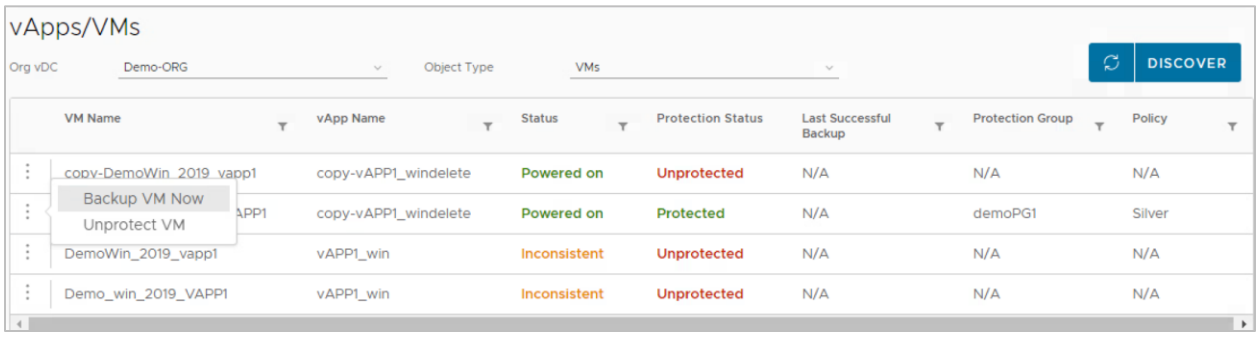
5. In the **Protect Object** window, click **Create New Group**. If you already have one, you can select an existing Protection Group instead. Enter the information as group name, start time, and policy, and click on **Save**.



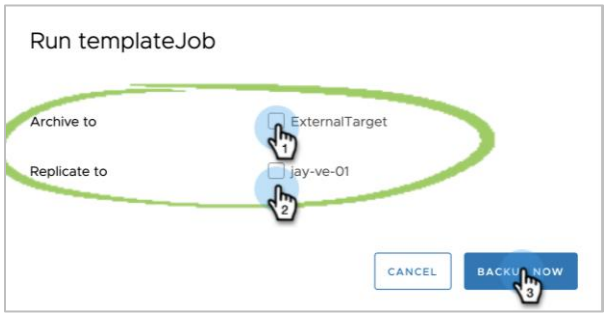
6. The VM's Protection Status has been updated to **Protected**. You can also log in to the Cohesity cluster to verify the protection group.



7. Once the object is protected, you can click the ellipsis (⋮) and either **Backup VM** (or **vApp** or **vApp Template**) **Now** or **Unprotect VM** (or **vApp** or **vApp Template**).



8. If you enabled **Allow Archival/Replication Target Selection** when you configured VCD above, you can specify the **Archive to** and **Replicate to** targets. After that, click **Backup Now**.

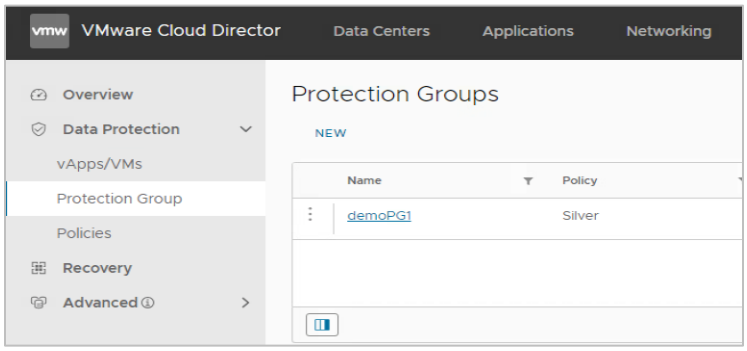


Protect Multiple Objects in a Single VCD Protection Group

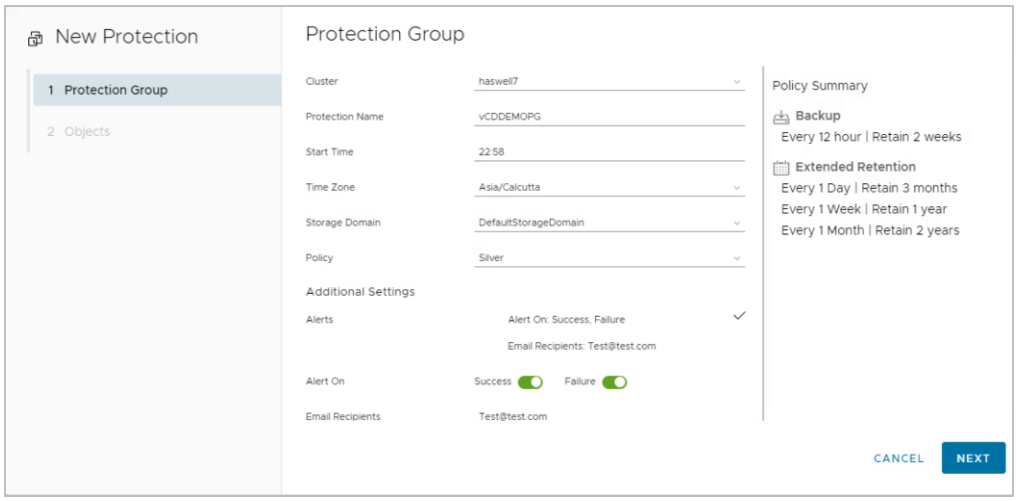
To protect multiple VCD resources in an organization, create a protection group via the VCD plugin. This method allows you to select multiple resources to be protected in a single VCD protection group.

To protect multiple VCD resources in the same VCD Protection Group:

1. Log in to VCD as the tenant user. Click the menu in the title bar and select **Data Protection**.
2. In the **Data Protection** menu, click **Protection Group** and click **NEW**.

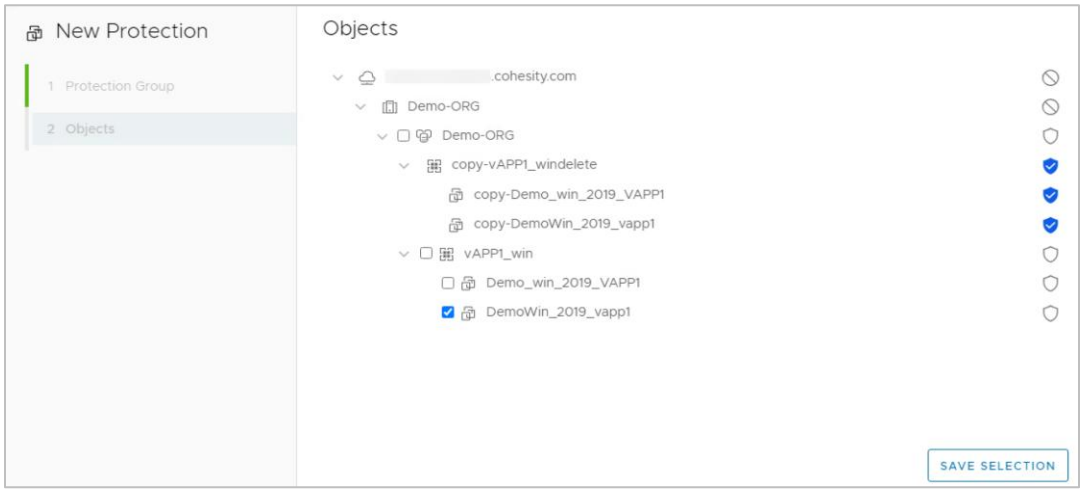


3. In the **New Protection** dialog, enter all the relevant information according to your requirements and click **Next** to select the objects to be protected. You can use options like setting **Email Recipients** to receive alerts for Protection Group **Success** and **Failure** runs.

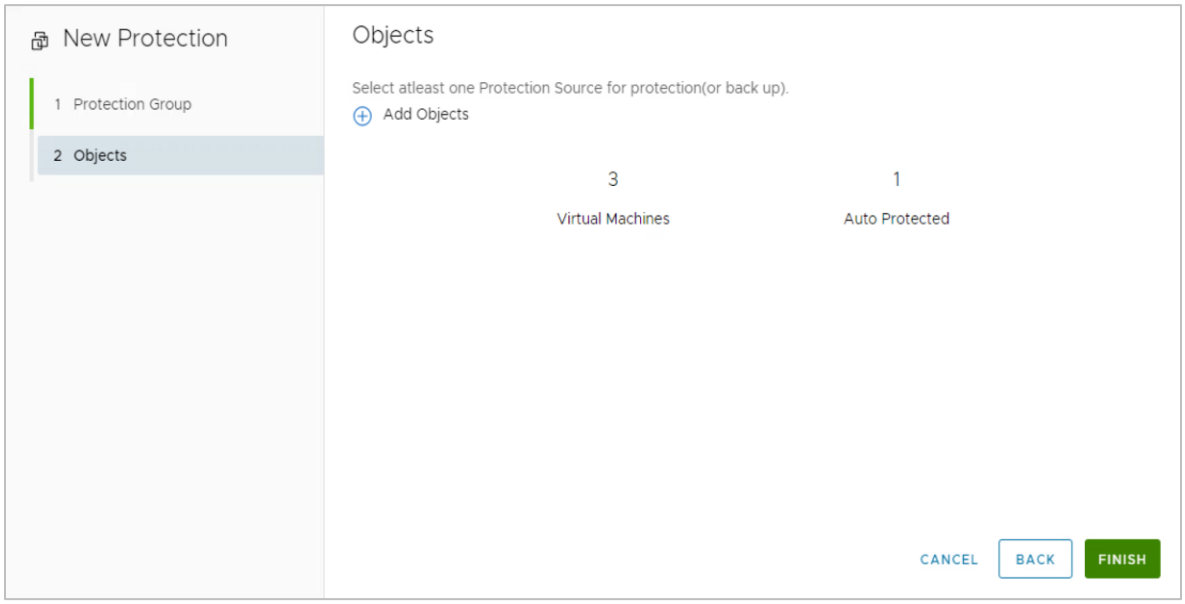


4. In the **Objects** page, click **Add Objects** to expand the VCD hierarchy tree. Here, you can protect the vApp, vApp Template, or VM. There is also an option to specify **Auto Protection** for a vApp or vApp template. If you choose **AutoProtect Object** (for a vApp or vApp Template), any VM that belongs to that object or any new VM created in that object will be protected automatically.

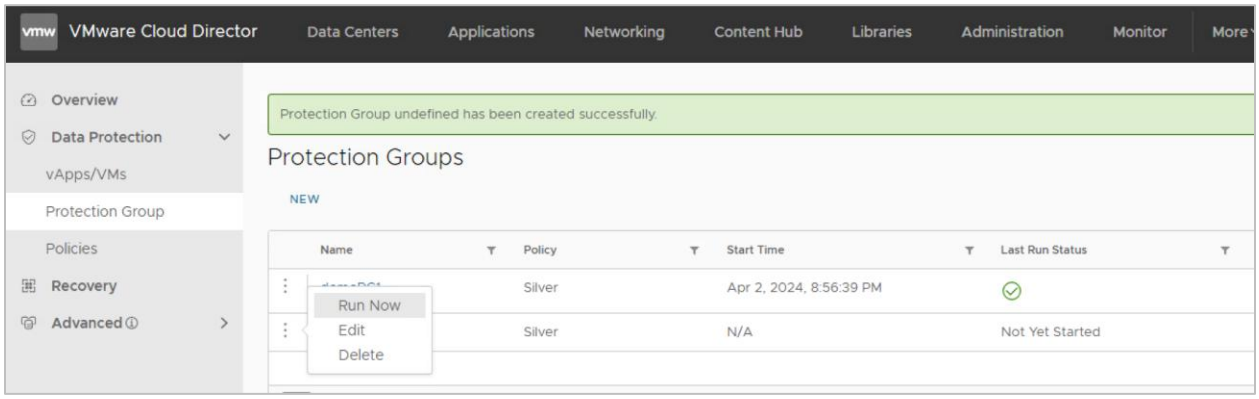
5. Select the objects to be protected and click **Save Selection**.



6. Review the protected objects and click **Finish** to create the VCD Protection Group.



7. Once the Protection Group is created, you can run the Group by clicking the ellipsis (⋮) and selecting **Run Now**. You can also edit the Protection Group to add or remove protection objects or change the configured parameters.



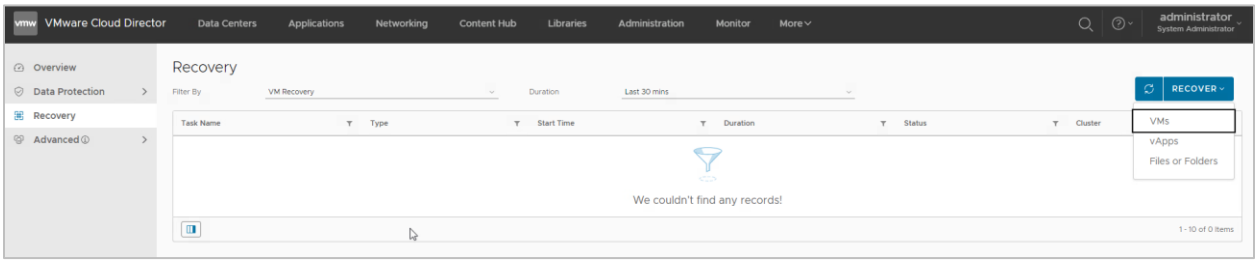
8. If you enabled **Allow Archival/Replication Target Selection** when you configured VCD above, you can specify the **Archive to** and **Replicate to** targets. After that, click **Backup Now**.

Restore VMs and vApps

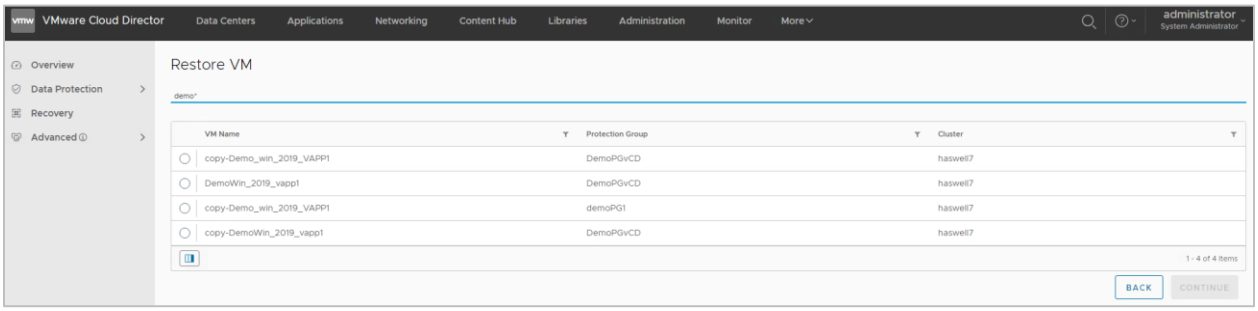
Cohesity provides granularity and flexibility to restore the VCD and its object as per the customer's requirement. You can recover VM, vAPP, vAPP templates, files, and folders as a self-service via the Cohesity VCD plugin to a state at a specified point in time.

To restore your VMs and vApps:

1. Log in to VCD as the tenant user.
2. Click the menu in the title bar and select **Data Protection**.
3. Click **Recovery** on the left. Under Recovery, you can filter by **VM Recovery**, **vApp Recovery**, **File Recovery**, or **File Download**. Choose the filter you need, click **Recover**, and then select **VMs** or **vApps**.



4. Search for the VM name that you want to recover. You can also use wildcard characters to search the VM. Select the VM that you want to recover and click **Continue**.

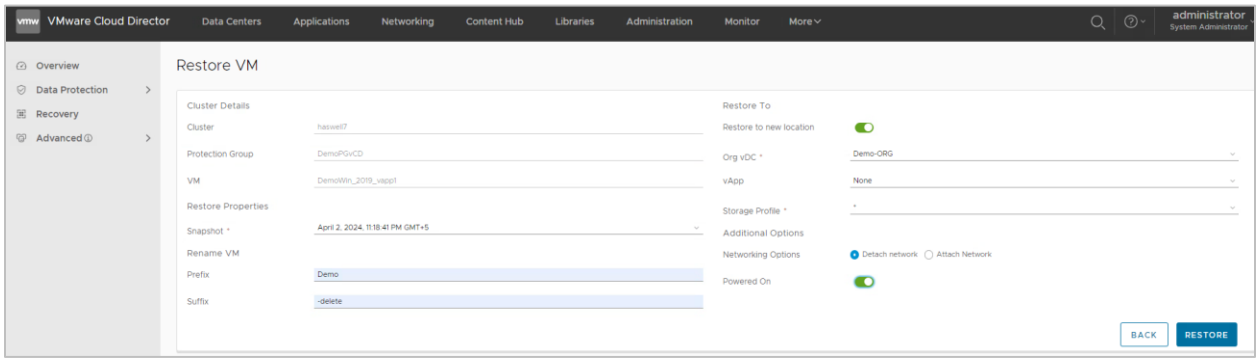


5. On the **Restore VM** page, select the **snapshot** you want to restore.

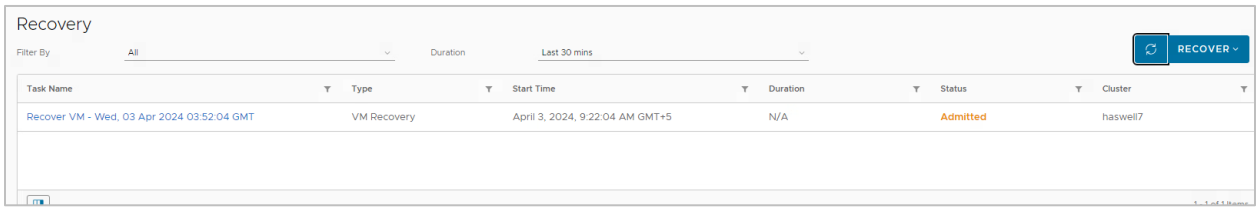
   There is an option to recover the VM to an **alternate location**, in this case, you will need to specify the target **Org vDC**, **vApp**, and **Storage Profile** as mentioned below.

   You can also attach the VM to an Org network by selecting **Attach Network** and entering the **Org Network name**. Enable **Powered On** to recover the VM in the On state.

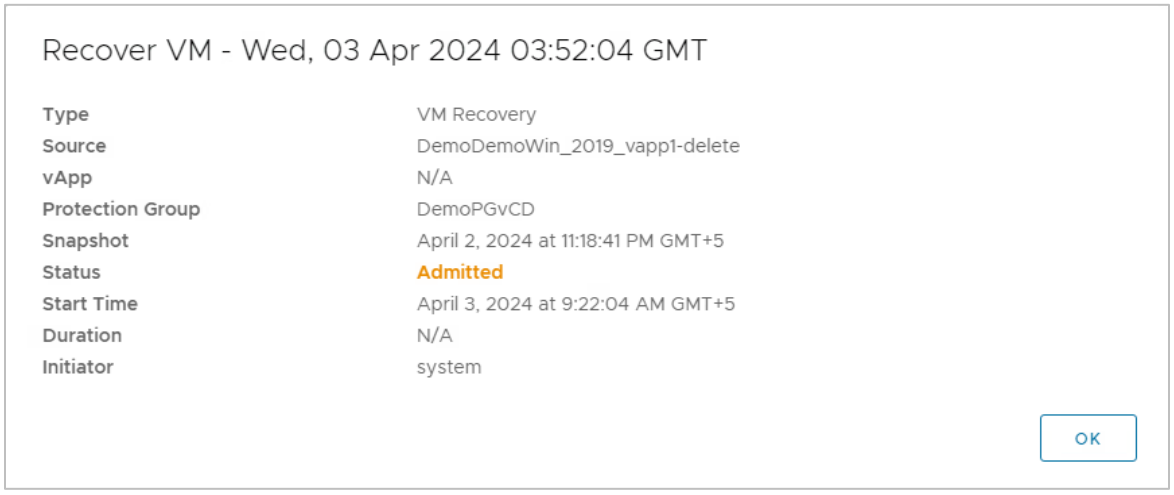
   Click **Restore**.



6. A recovery task is created, which you can monitor on the **Recovery** page. You can refresh the page to check the updated status of the recovery task. The status can be **Admitted**, **InProgress**, **Failure**, or **Success**.



7. You can click on the recovery task to see the details.

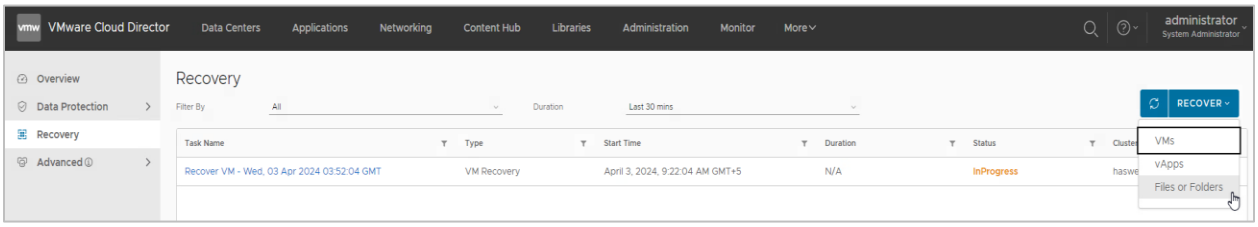


Restore or Download Files and Folders

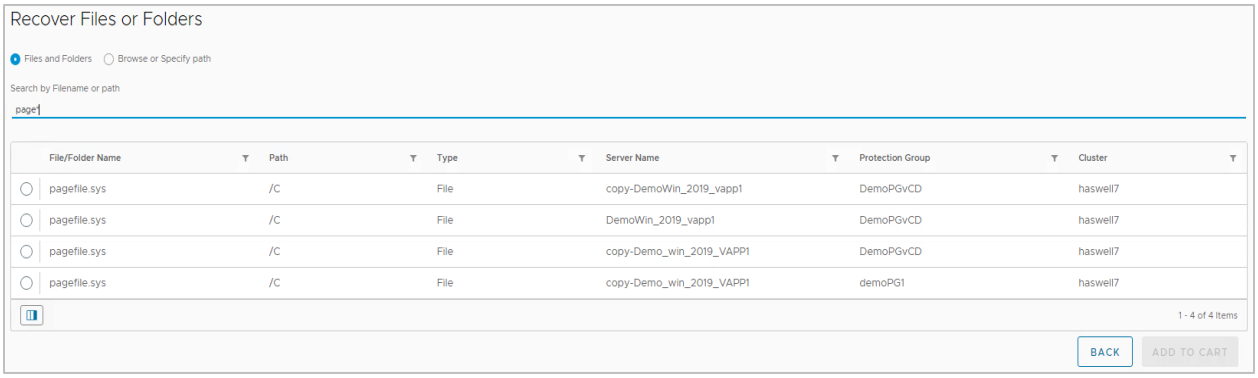
Cohesity supports the granular restore of the VCD environment, as you can restore files and folders using backup snapshots via the VCD plugin as a self-service model. This way, a user can search for a required file, browse through the directory structure, and recover any file or folder by choosing from the available snapshots.

To restore a file or folder:

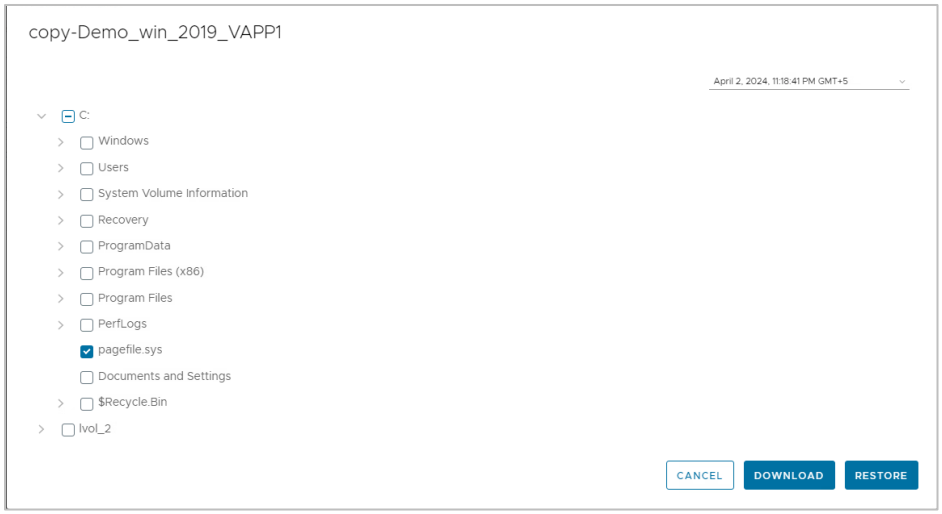
1. Log in to VCD as the tenant user.
2. Click the menu in the title bar and select **Data Protection**.
3. Click **Recovery** on the left. Under Recovery, you can filter by **VM Recovery**, **vApp Recovery**, **File Recovery**, and **File Download**. Choose the filter you need, click **Recover**, and then select **Files or Folders**.



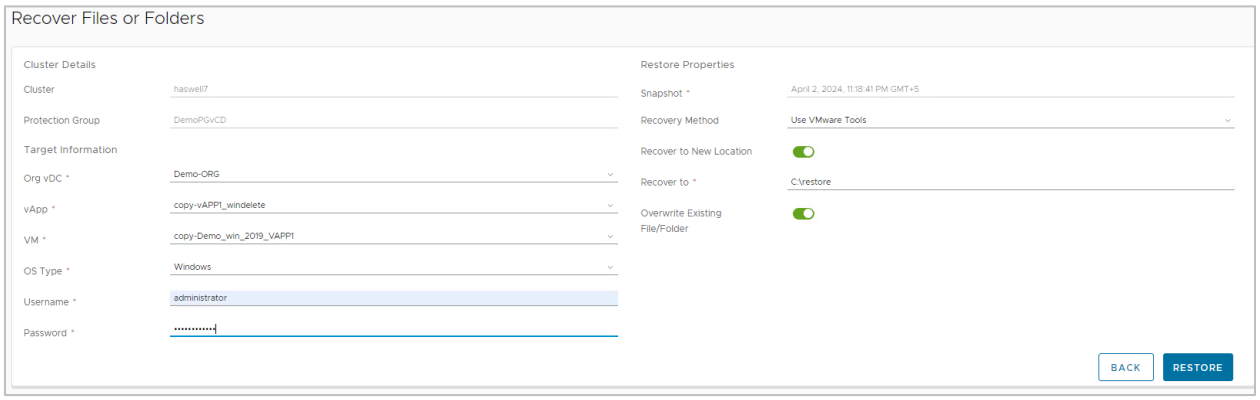
4. Select **Files or Folders** and enter a string to search for the file or folder that you want to recover. If you are not sure of the exact name, you can use the wildcard '*'. Select the file that you want to recover and click **Continue**.



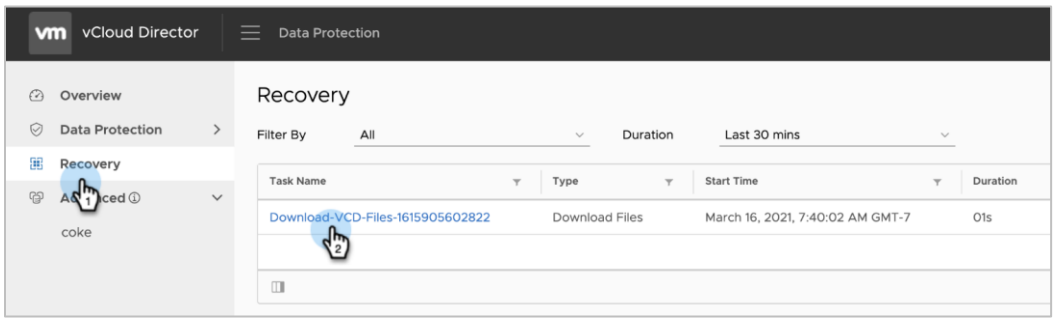
The second option the Cohesity VCD plugin provides is to **Browse or Specify the path** from the filesystem browser, select the file you want to recover, and click **Continue.** You can select the recover point from the top right drop-down menu.



5. Specify the OS credentials and the recovery method you want to leverage as VMware tools or Cohesity agent. If you are choosing an alternate location, you must specify it and the overwrite option. Click **Restore.**



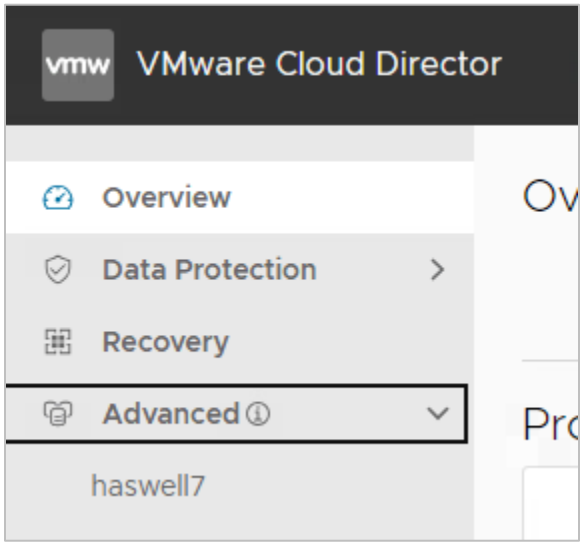
6. A recovery task is created, which you can find under the **Recovery** page. Once the recovery task is complete, you can click **Task Name** to download the file.



Cross-Launch Cohesity UI from VCD Plugin

Cohesity provides the functionality to log in to the organization portal of the Cohesity UI. With a single click, you can log in to the Cohesity UI and the Cohesity organization mapped with the VCD organization. If you enable **Cluster Access** for the current tenant when configuring VCD, you can navigate to the Cohesity cluster by clicking **Advanced** and then the Cohesity Organization name.

Figure 6: Cross-Launch Into Your Cohesity Organization



Appendix A: Terminology

It's important to understand some key terms and concepts in VCD and Cohesity multi-tenancy:

- **Cohesity Organization**. In the context of Cohesity, the multi-tenancy feature is called organizations. Each tenant on a Cohesity cluster is called an organization.
- **VCD Organization**. Similar to Cohesity, VMware Cloud Director supports multi-tenancy through the use of Organizations. In VCD, an organization is a unit of administration for a collection of users, groups, and computing resources. Users authenticate at the Organization level, supplying credentials established by an organization administrator when the user was created or imported. System administrators create and provision Organizations, while Organization administrators manage Organization users, groups, and catalogs.
- **vApp**. vApp is a virtual system that contains one or more individual virtual machines and parameters that define operational details.
- **vApp Template**. A vApp Template is a virtual machine image loaded with an operating system, applications, and data. These templates ensure that virtual machines are consistently configured across an entire Organization.
- **Organizational Virtual Datacenter (vDC)**. An organization virtual datacenter (vDC) in VCD provides resources to a VCD organization and is partitioned by a provider vDC. VCD Organization vDCs provides an environment where you can store, deploy, and operate virtual systems.

  NOTE: A single Organization can have multiple Organization vDCs.

- **VCD Catalog**. VCD Organizations use catalogs to store vApp Templates and media files. The members of an organization who have access to a catalog can use the catalog's vApp Templates and media files to create their own vApps. A system administrator can allow a VCD Organization to publish a catalog to make it available to other Organizations. These VCD Organizations' administrators can choose which catalog items to provide their users.

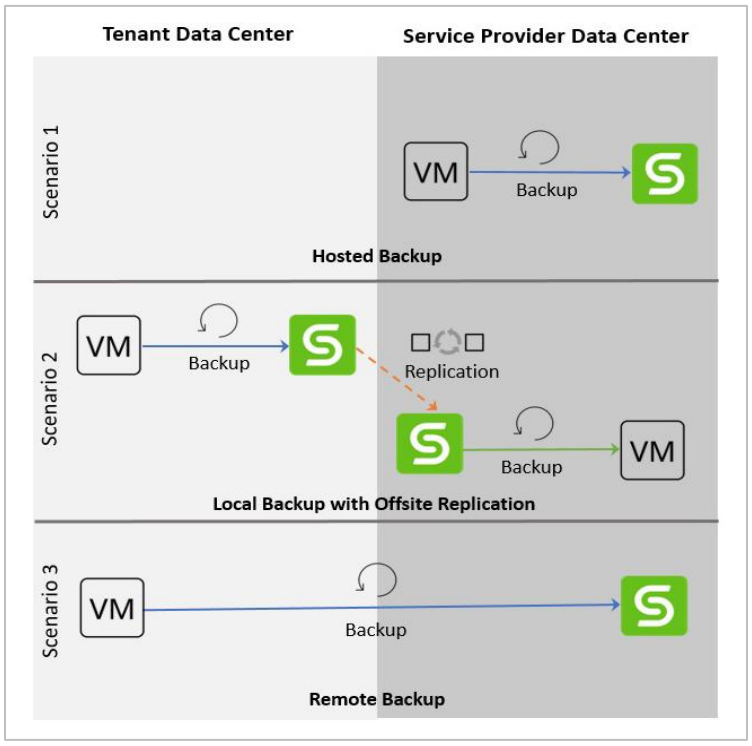
Appendix B: Deployment Options for Cohesity VCD Protection

Backup-as-a-Service (BaaS) refers to the approach of taking backups of a customer's IT infrastructure by leveraging the backup service provided by a service provider. Service providers often have a multi-tenant infrastructure wherein they can back up data from multiple customers to a shared underlying infrastructure while logically isolating those backups for each customer.

There are several different scenarios through which a service provider can deploy BaaS as an offering to their tenant customers:

- **Scenario 1**: Hosted Backup (supports the VCD workflow in this guide)
- **Scenario 2**: Local Backup with Offsite Replication
- **Scenario 3**: Remote Backup

Figure 7: Cohesity's Backup-as-a-Service Deployment Options for SPs



To go over all the possible scenarios, see the Backup as a Service Technical Solutions Guide.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sadik Sayed is a Snr. Solution Architect at Cohesity. In his role, he focuses on Virtualization Data Protection — VMware vSphere, VMware Cloud Director, VMware Cloud Foundation, Microsoft HyperV and Nutanix AHV.

Other essential contributors include:

- Gautam Bhasin, Director Product Management
- Mithun Shitole, Staff Engineer

Document Version History

VERSION	DATE	DOCUMENT HISTORY
2.2	April 2026	7.4 updates
2.1	Feb 2026	7.3 updates
2.0	May 2024	Updated Version
1.0	June 2021	First complete document

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.