COHESITY

# Backup as a Service Technical Solutions Guide

Version 3.3

Nov 2025

**ABSTRACT**

*Cohesity provides a web-scale, software-defined architecture that is perfect for service provider deployments. Cohesity offers many out-of-the-box features that enable service providers to create compelling, differentiated, and efficient solutions, leading to enhanced customer offerings, experiences, outcomes, and better revenue. Use this guide to learn how you can leverage Cohesity's multi-tenancy features to provide a compelling Backup as a Service solution.*

# Table of Contents

# Figures

# Tables

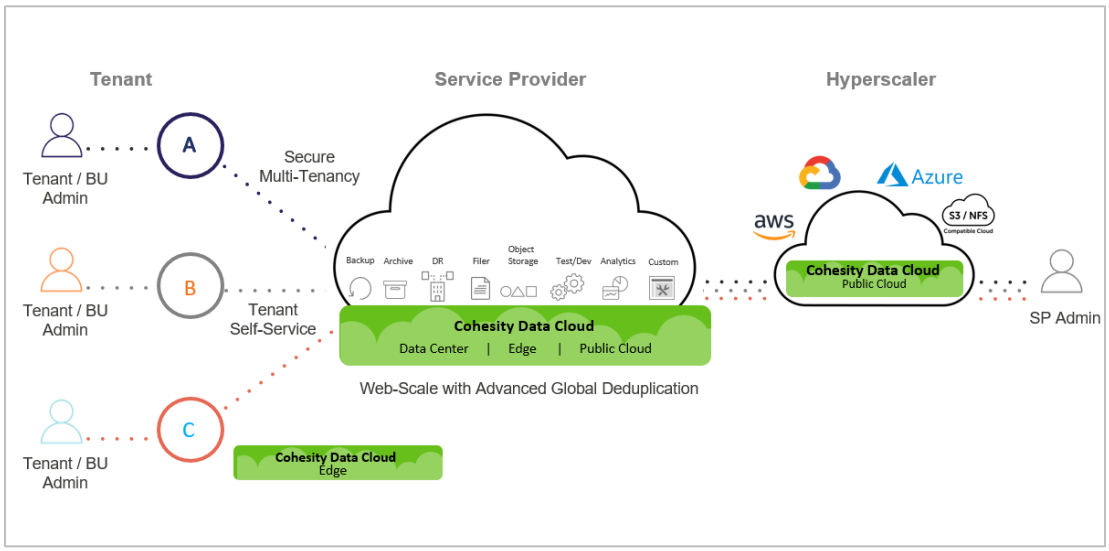




# Introduction to Backup as a Service

Multi-tenancy opens the door to many advantages for service providers, such as investment efficiencies, security, and data isolation. Secure multi-tenancy is a crucial part of planning corporate IT infrastructure today, and providing security guardrails is built into the core architecture of Cohesity. With Cohesity, service providers can create an “Organization” corresponding to each tenant customer on the Cohesity cluster.

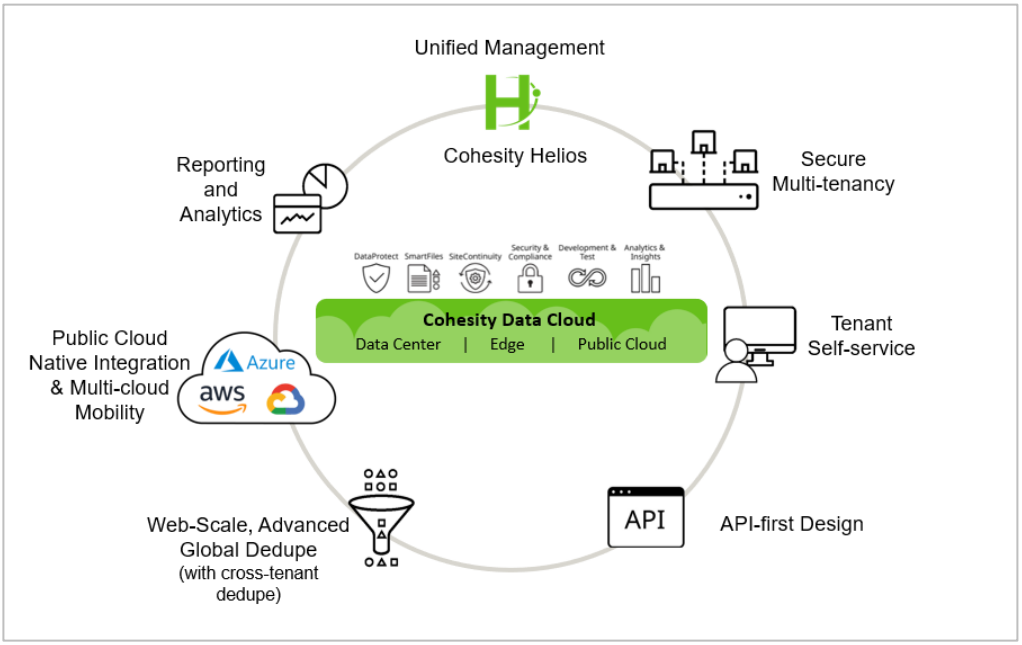
Figure 1: Deliver Backup as a Service Using Cohesity’s Secure Multi-tenancy



# Features and Benefits

The Cohesity platform is built with service providers in mind. Figure 2 below showcases the Cohesity features that dramatically enhance service provider deployments.

Figure 2: Key Cohesity Features for Service Providers




Among the benefits offered by this approach are

- **Unified Management**. Helios is Cohesity's SaaS-based management platform that provides a single view and global management of all your Cohesity clusters, whether on-premises in the cloud, or Virtual Edition, regardless of cluster size. You can quickly connect clusters to Helios and then access them from anywhere using an Internet connection and your Cohesity Support Portal credentials.

  Helios provides:

  - **Multi-cluster management**. Actively manage all your clusters, including multi-cluster monitoring, reporting, and orchestrated upgrades, from a single dashboard.
  - **Global actionable search**. Search across clusters and take action right from the search results. For example, search for all unprotected VMs and create jobs to protect them.
  - **SmartAssist**. Automatically schedule and orchestrate jobs and workloads to help meet your SLAs. Get recommendations based on capacity forecasting and disk failure prediction. View important Cohesity field notices.
  - **Cloud Edition**. Deploy Cloud Edition clusters using Helios.
- **Secure Multi-tenancy**. Enable secure multi-tenancy to provide a logical separation between the multiple tenants hosted on your Cohesity cluster. Each tenant is represented in Cohesity as an o*rganization*.
- **Tenant Self-Service**. Configure role-based access control (RBAC) to provide role-based access to the employees *within* each tenant organization.
- **API-first Design**. Cohesity Platform's API-first design enables automation and orchestration for almost all the workflows available on the cluster.

- **Web-Scale, Advanced Global Deduplication**. Cohesity Platform is built on a web-scale architecture. This not only provides greater operational scalability, but also greater storage efficiency thanks to our advanced global deduplication.
- **Public Cloud Native Integration and Multi-Cloud Mobility**: Cohesity Platform has native public cloud integrations and provides multi-cloud mobility, making it straightforward to keep extending your system's capacity and capabilities.
- **Reporting and Analytics:** Cohesity gives service providers access to usage metrics to help them implement chargeback. Service providers can retrieve and analyze these metrics via:
  - **Built-in Reports**. Accessible in the Cohesity browser UI. See Reports in the online Help.
  - **Custom Reports**. Generated using:
    - The Cohesity REST API.
    - The Custom Reporting Database. See the Cohesity Custom Reporting Solution Guide.
    - API Access from the cluster and Helios.

## Terminology

The following terminology is important to understand as you learn about deploying Backup as a Service (BaaS) for your tenant organizations.

Table 1: BaaS Terminology

| Terminology | Description |
|---|---|
| AD | Active Directory |
| BaaS | Backup as a Service |
| Cross-Connect | A cross-connect is a point-to-point cable link between a customer and a service provider. |
| DNS | Domain Name System |
| Hybrid Extender (HyX) | Hybrid Extender is a proxy that is deployed on the tenant vCenter and helps to set up a secure TCP/IP channel between the tenant's local network and the Cohesity cluster sitting in the service provider's environment. |
| Hybrid Extender V2 (HyXV2) | Hybrid Extender V2 launched in version 6.6, and it has dual home configuration. |
| Network Realm | Network Realm ensures source-level selection in a multi-tenant environment and allows you to create and manage multiple isolated networks within a tenant. |
| IaaS | Infrastructure as a Service |

| Terminology | Description |
|---|---|
| LACP | Link Aggregation Control Protocol, as defined in the IEEE 802.3ad specification. |
| Multi-tenancy | An architecture in which a single instance is shared across multiple clients who are logically isolated from each other while being physically integrated. |
| NIC | Network Interface Card. Indicates a single network link on the node used to connect to other devices. |
| NTP | Network Time Protocol |
| Organization ID | The Organization ID is the multi-tenancy identifier for each tenant organization on a service provider's Cohesity cluster.<br>**NOTE**: The Organization ID is a short string that is used for logins in the form of **<***User***>**@<*Organization_ID*>. It can include no more than eight alphanumeric characters and must be unique in the system. |
| RBAC | Role-based access control |
| TCP | Transmission Control Protocol |
| Virtual IPs (VIPs) | An IP address that does not correspond to an actual physical network interface. Cohesity recommends you use one VIP for each node in your Cohesity cluster. |
| VLAN | Virtual Local Area Network |
| VPN tunnel | A VPN is a Virtual Private Network. Use a VPN tunnel to connect two private networks across public networks. |
| Tenant Self-service | Tenant admins/users can recover the data themselves. |
| gRPC | gRPC is a modern open-source high-performance Remote Procedure Call (RPC) framework that can run in any environment. |

# BaaS Features for Service Providers

Service providers need some crucial capabilities to provide any solution “as a Service.” Table 2 below outlines these essential service provider requirements and explains how to achieve them using native features in Cohesity, for example, isolation w.r.t data, network, and access. We discuss these in further detail in the subsequent chapters.

Table 2: Native Cohesity Features for BaaS

| Feature | Detail |
|---|---|
| Organization management and isolated namespaces<br>Secure Multitenancy | • Administrators can provision organizations and assign them Cohesity resources (storage domains, VLANs, IP address ranges, Active Directory domains, etc.).<br>• Role-Based Access Control allows tenant administrators to control what’s visible to their users.<br>• Cluster-level administrative capabilities are hidden from, and unavailable to, tenant organizations.<br>• For data protection, each organization privately owns its Sources, Protection Groups, index, search, and reports. |
| Network isolation | • **Network**: You can isolate tenant organizations from each other by assigning each its own VLAN or IP address range to benefit network isolation for in-flight data.<br>• **Data**: You can also isolate tenant organizations from each other logically by assigning each organization its own storage domain, which creates separate, independent deduplication domains and encryption keys. |
| Reporting for each tenant organization | • For chargeback purposes, organizations can see their own storage consumed.<br>• For service provider administrators, there’s a new report called “Storage Consumed by Organizations,” which lists all tenant organizations, their storage domains, and the data consumed in each.<br>• The new “Customized Reporting - DB” can also meet this need with even greater flexibility |
| Efficient storage usage per tenant | • Service providers can achieve even higher storage efficiency rates by choosing the option to configure tenants to share the same storage domain, which acts as a single deduplication domain, across tenant data, while access is still limited to each. |

| Feature | Detail |
|---|---|
| Impersonate tenant organizations to diagnose and debug problems | • Service provider users can “impersonate” organization users and thereby preview and verify what their tenant customers see in order to help customers diagnose and debug issues.<br><br>Examples of impersonation include:<br>○ Service provider *administrator* acquires tenant *administrator* privileges during impersonation.<br>○ Service provider *operator*s acquire tenant *operator* privileges during impersonation.<br>○ Service provider *viewers* will get tenant *viewer* privileges during impersonation.<br>• To ensure maximum security, all actions taken under impersonation are audit-logged with the authentic user’s identity (not the impersonated identity) and are visible to the tenants and the service provider. |
| Tenant Self-Service | • Tenant users will be able to perform self-service of backup and restore with RBAC Controls. |
| Efficient backup and restore workflows | • Cohesity provides efficient backup and restore workflows, which helps service providers manage large environments with multiple workloads using a single pane of glass. |
| Long Term Archival Service | • Service Providers will be able to provide Archival as a Service, without needing additional silos of infra. |
| Data encryption and key management | • Cohesity has a built-in key manager that generates keys and stores them internally on the SSDs in encrypted form.<br>• Data on the cluster is encrypted using a Data Encryption Key (DEK) and the DEK is in turn encrypted using a Key Encryption Key (KEK). The encryption/decryption process is done within the Cohesity cluster and is transparent to all inbound/outbound protocols and applications, such as backup, archiving, and file services. Also, the keys are stored in a distributed fashion to be resilient in the rare event of a hardware failure.<br>• The default key rotation policy for KEK is 90 days, but the administrator can configure a different value. |

| Feature | Detail |
| --- | --- |
| Third-party integration | • Cohesity Platform is based on an API-first architecture, valuing automation, consumable APIs, and self-service capabilities from the get-go. Users can enjoy error-free consistency and self-service manageability that extends the capabilities of individual applications and enables IT to spend less time with management, and more time with ambitious, value-oriented projects.<br>• Supported automation frameworks include:<br>  ○ VMware vCloud Director<br>  ○ VMware vRealize Automation (vRA) and Orchestration (vRO)<br>  ○ ServiceNow<br>  ○ Python/Powershell SDK |

# Deployment Scenarios

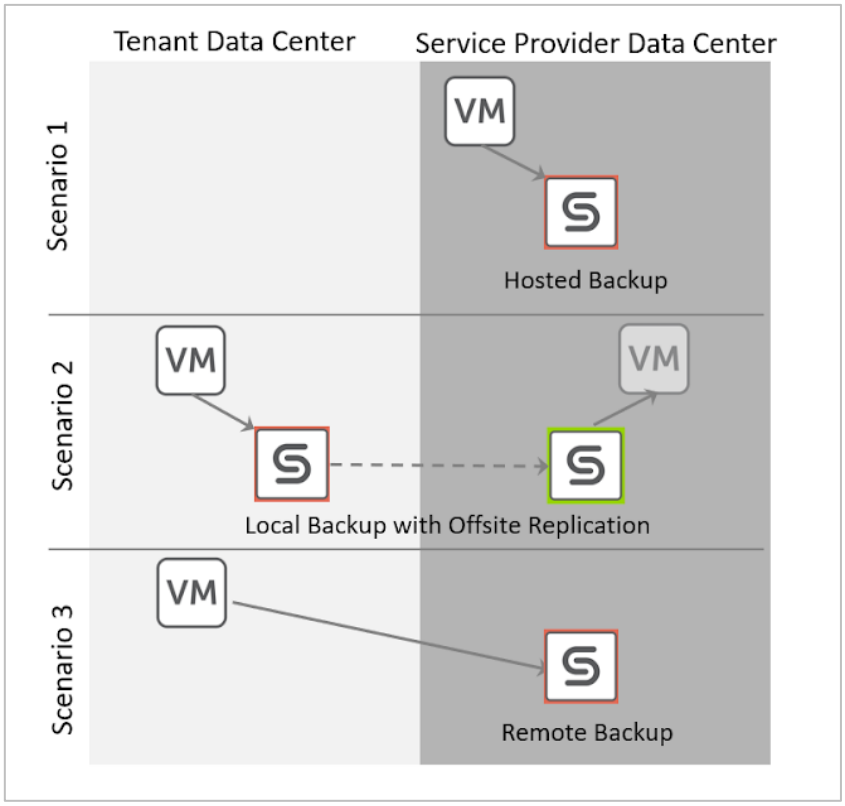
Backup as a Service refers to the approach of taking backups of a customer's IT infrastructure using the backup service provided by a service provider. Service providers often have a multi-tenant infrastructure wherein they can back up data from multiple customers to an underlying shared infrastructure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

There are many different scenarios through which a service provider can deploy BaaS as an offering to their tenant customers. In this document, we discuss the three most common deployment scenarios:

Table 3: Deployment Scenarios

| Service Provider Deployment Scenarios | Description |
|---|---|
| Scenario 1: Hosted Backup | Service Provider provide shared hosted infrastructure as a service (IaaS) wherein they host the customer's IT infrastructure. |
| Scenario 2: Local Backup with Offsite Replication | To Leverage the Disaster Recovery, the customer keeps the primary copy on-premise and replicates the secondary copy to the central service provider location. |
| Scenario 3: Remote Backup | The service provider provides the Backup as a Service over the LAN/WAN/MAN/Internet connectivity. Customer and Service providers are in remote locations. |

Figure 3: BaaS Deployment Scenarios




:

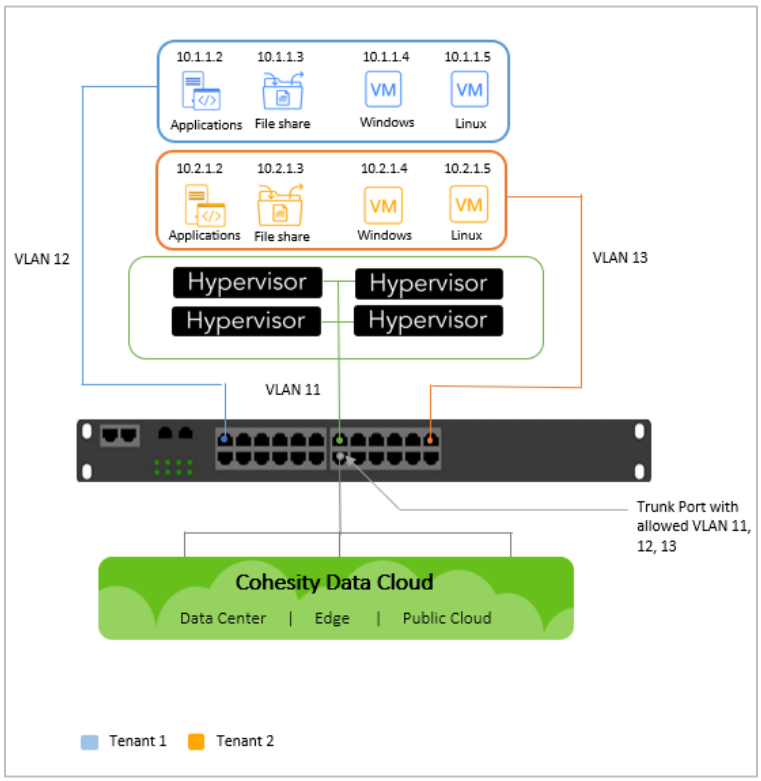
## Hosted Backup Deployment

Service providers often provide shared hosted infrastructure as a service (IaaS) wherein they host the customer's IT infrastructure. Cohesity Platform provides them with the ability to offer their customers BaaS in a *secure* multi-tenant environment. Hosted backup is typically implemented in one of two network topologies, a tenant-reachable or tenant-isolated network, depending on existing infrastructure and business requirements.

## Tenant-reachable Network

- **Unique IP address across tenants**. In this scenario, the VMs across the tenants have unique IPs. Cohesity can identify and reach the VMs using those unique IPs.

  Figure 4: Hosted Backup on Tenant-reachable Network with Unique Tenant IP




- **Overlapping IP addresses across tenants**. In this scenario, the VMs across the tenants have overlapping IPs. Cohesity Platform is unable to identify the VMs using those overlapping IPs but *can* reach the VMs using NAT (Network Address Translation) IP mappings. For Linux file-level restores from a mounted Cohesity View, you can use the solution for overlapping IP addresses in tenant-isolated networks below.

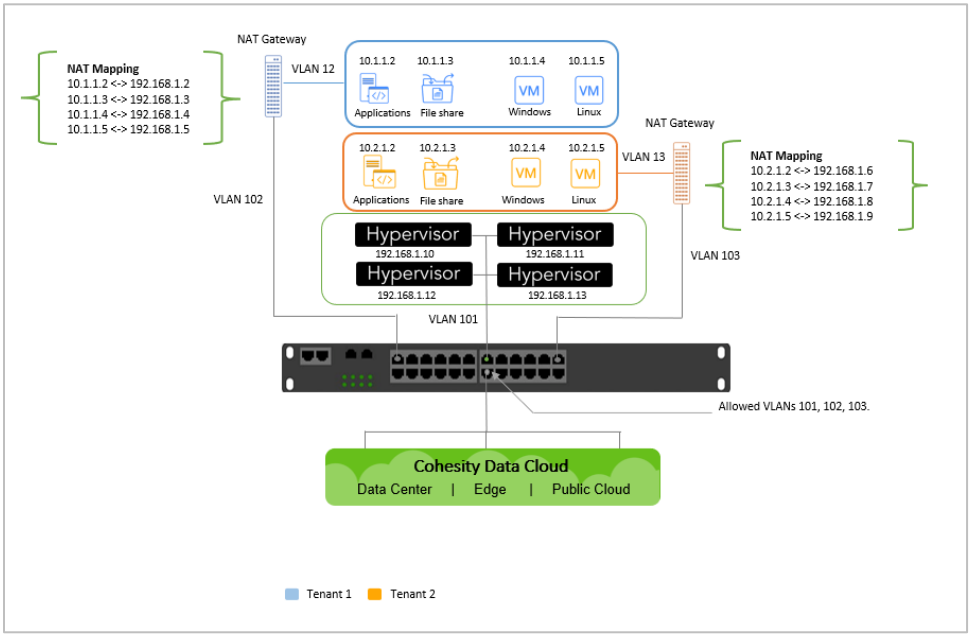
> **NOTE**: Cohesity uses VMware tools to perform Linux file-level and folder-level restores. As a result, connectivity to VMs is not mandatory for Linux file level restores.
>
> Hybrid Extender V2 can be used to avoid NAT configuration. See Remote Backup Deployment.

## Tenant-isolated Network

Your network topology is tenant-isolated when each node in the Cohesity cluster can communicate with the vCenter, but *not* with the individual VMs in the tenant network. This network also has two variations:

- **Unique IP address across tenants**. In this scenario, the VMs across the tenants have unique IPs. However, the Cohesity cluster is unable to reach the VMs using the unique IPs directly. Instead, the Cohesity cluster accesses the VMs through a NAT gateway.

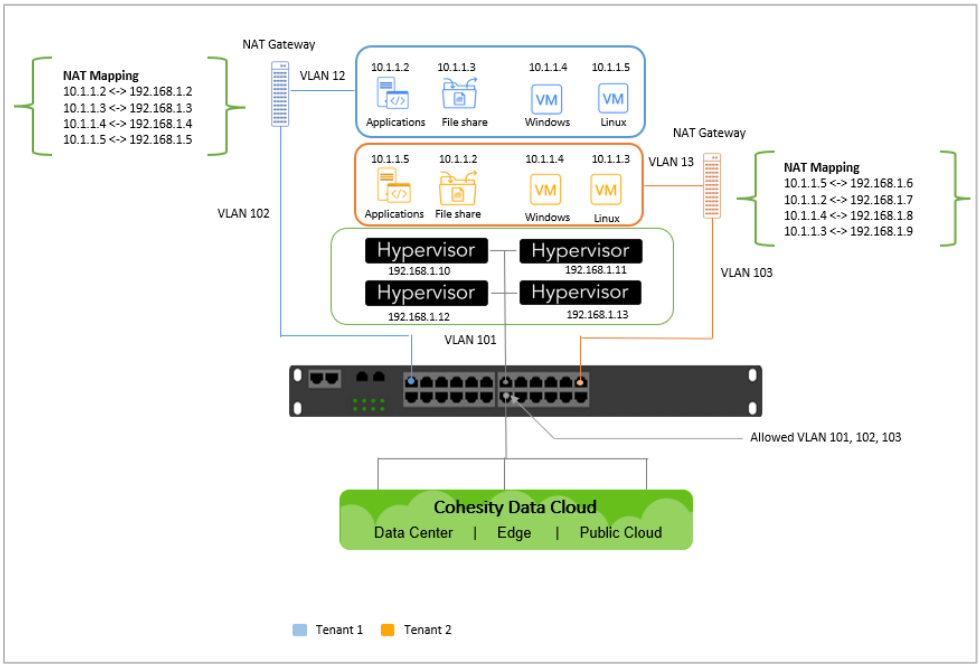
  Figure 5: Hosted Backup on Tenant-isolated Network with Unique Tenant IPs




**NOTE**: Hybrid Extender V2 can be used to avoid NAT configuration. See Remote Backup Deployment.

- **Overlapping IP addresses across tenants**. In this scenario, because VMs across the tenants have their own private networks, they can have the same IP ranges. They may have overlapping IPs. The Cohesity cluster cannot reach the private network and is unable to uniquely identify or reach the VMs using their IPs. Because the IPs are overlapping, the Cohesity cluster accesses the VMs using NAT gateways.

Figure 6: Hosted Backup on Tenant-isolated Network with Overlapping Tenant IPs




**NOTE**: Hybrid Extender V2 can be used to avoid NAT configuration. See Remote Backup Deployment.

## Hosted Backup: Supported Workloads

The supported workloads for Hosted Backup are:

- ESXi/vCenter/vCloud Director
- HyperFlex
- Hyper-V VM Servers
- AHV
- Physical Servers
- MS SQL VM, FCI, AG
- Oracle Standalone, Oracle RAC
- SAP HANA
- SAP Sybase ASE
- Remote Adapters
- NAS Backup (Netapp, Isilon, Generic NAS)
- Cohesity Views
- Microsoft Active Directory, Microsoft Exchange OnPrem
- Office 365
- AWS Cloud WorkFlows

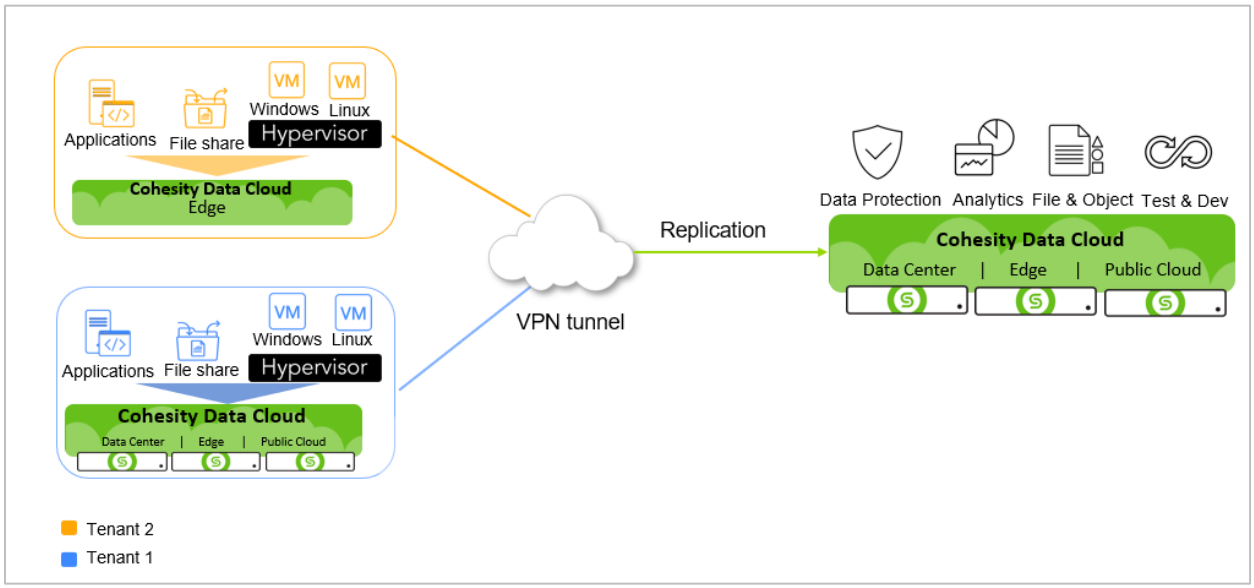
For more information, see supported Multitenancy Workflows.

# Local Backup with Offsite Replication Deployment

Service providers can provide managed BaaS for customers who prefer to keep the primary copy of the backup data on-premises and then replicate a copy of the backup to a central service provider location (similar to tape offsiting) for disaster recovery (DR) purposes.

To that end, service providers can deploy Cohesity Virtual Edition (VE) or Physical Clusters into the tenant environment to take the backups locally and then replicate (or archive) the backup snapshots to the central location.

Figure 7: Local Backup and Offsite Replication to Service Provider Data Center




## Local Backup: Supported Workloads

The supported workloads for managed BaaS with data center replication are available in Supported Software in the online help. However, when it comes to offsite replication, only the following Multi-tenancy Qualified Workloads are supported.

- ESXi/vCenter/vCloud Director
- HyperFlex
- Hyper-V VM Servers
- AHV
- Physical Servers
- MS SQL VM, FCI, AG
- Oracle
- SAP HANA
- SAP Sybase ASE
- Remote Agents
- NAS Backup (Netapp, Isilon, Generic NAS)

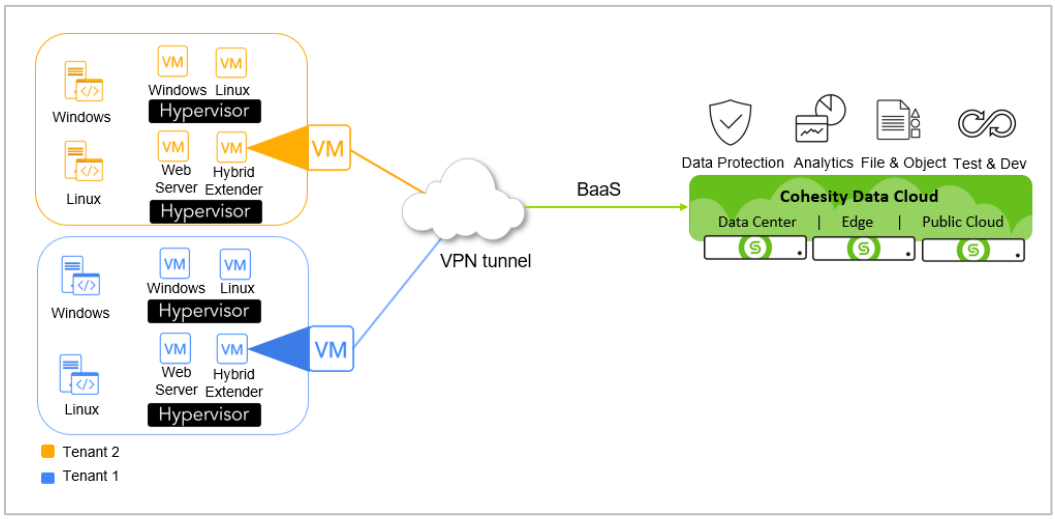
- Cohesity Views
- Microsoft Active Directory, Microsoft Exchange OnPrem
- Office 365
- AWS Cloud WorkFlows

## Remote Backup Deployment

Using Cohesity Platform, service providers can provide BaaS over the LAN/WAN/MAN/ internet. In such scenarios, the backup and restoration times depend on the network bandwidth and latency between the tenant source and Cohesity cluster.

In our example below, Cohesity's Hybrid Extender in the tenant's virtualized environment is acting as a proxy to all traffic traveling to the Cohesity cluster for backup. This scenario is particularly relevant when the service provider must support overlapping IP addresses or an isolated tenant network. For more, see Use the Hybrid Extender to Manage Tenant Network Connections below.

Figure 8: Remote Backup




## Remote Backup: Supported Workloads

The supported workloads for Remote Backup are:

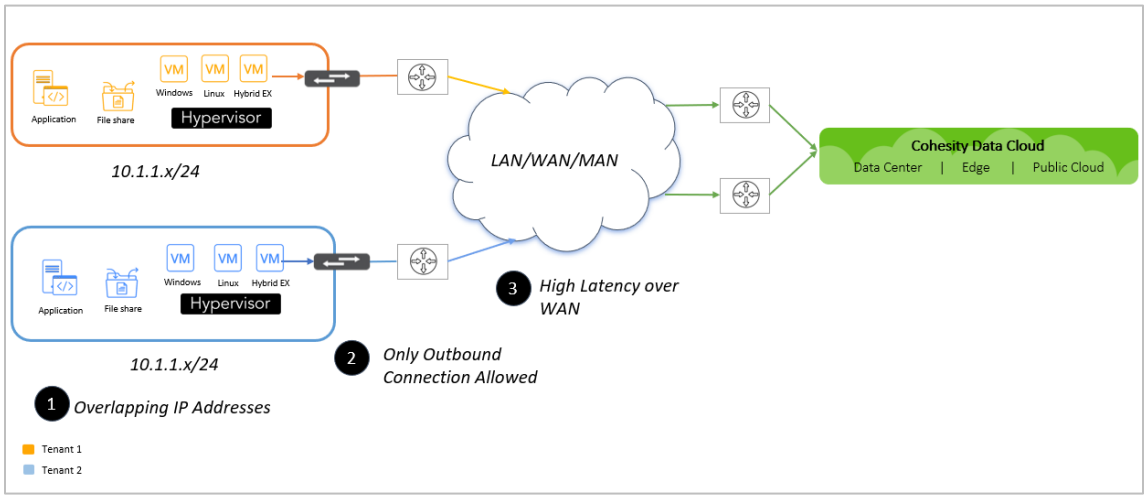
- VMware ESXi/vCenter
- Physical servers
- MSSQL VM, FCI, AG
- Oracle
- SAP HANA
- SAP Sybase ASE
- NAS (Generic NAS, Isilon)

For more information, see Supported Multitenancy Workflows for Hybrid Extender.

# Use the Hybrid Extender to Manage Tenant Network Connections

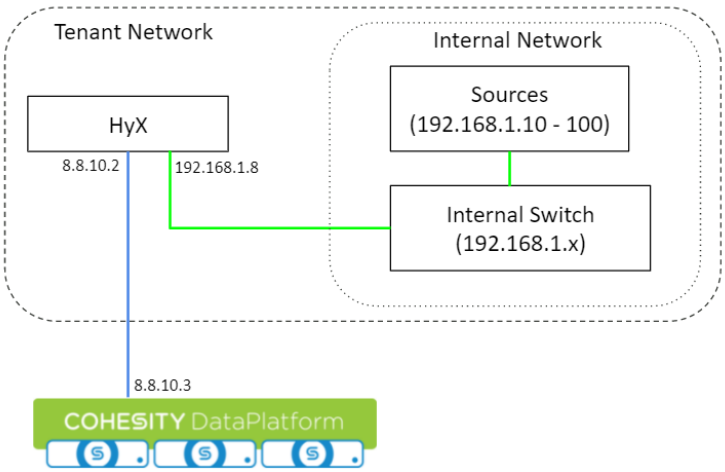
Backup as a Service can be deployed in different ways depending upon the location and network connectivity between the service provider and the tenants. In a real-world scenario, service providers are often faced with a situation wherein their customers have the same IP address ranges, subnets, and isolated identical networks. A remote connection requires opening dedicated incoming ports on the tenant firewalls in some situations. To enable service providers to host multiple customers with the same IP address ranges and subnets on the same Cohesity cluster and provide a proxy that connects to the Cohesity cluster, Cohesity has introduced a component called the Hybrid Extender. It acts as a proxy VM between the organization and Cohesity cluster and provides Source-side deduplication. It communicates over a secure gRPC tunnel and is encrypted using mutual TLS1.2.

Figure 9: Cohesity Hybrid Extender Streamlines Tenant Network Management




Cohesity Introduced Hybrid Extender V2 with Cohesity cluster 6.6. The main feature of HyX V2 is that it is dual-homed.

- HyX V2 is a dual Home. It can simultaneously communicate to tenant private Network and Service Provider Network (outside of tenant organization).
- You can configure the Hybrid Extender using one or two network interfaces. Each network interface can be configured with DHCP or static IPs. DHCP is the default. Static IPs will be used only if you configure a static IP.
- Dual Home eliminates the network configuration changes (such as NAT mappings/VLANs/ VPNs or changing firewall rules) between Hybrid Extender and Cohesity cluster compared to HyX V1.
- HyX V2 added support for additional adapters and enabled mount-based restores using HyX. (Earlier sources need to connect directly to the cluster to perform mount based restores)
- It has two network interfaces
    - Primary Interface (ens160) --> Communicates with Service Provider Cohesity Cluster
    - Secondary Interface (ens192) --> Communicates with Tenant's internal network




The Hybrid Extender performs several vital functions:

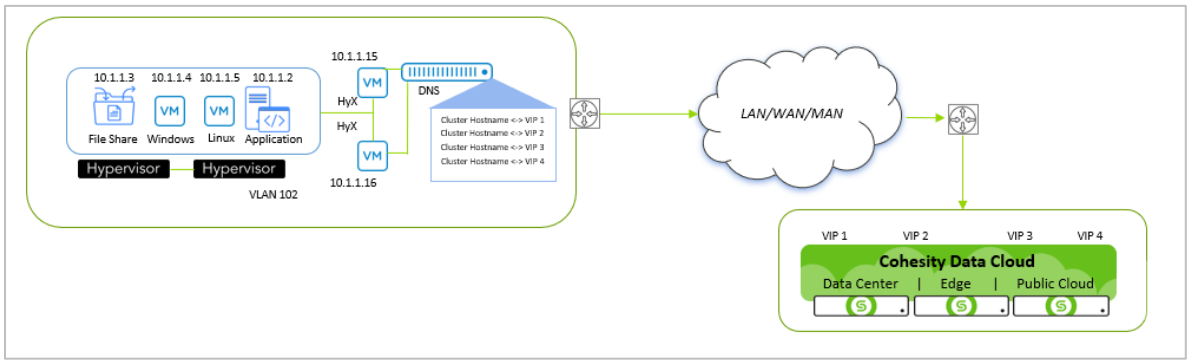
- **Secure TCP/IP**. It is a proxy that is deployed on the tenant VMware vCenter and helps to set up a secure TCP/IP channel between the tenant's local network and the Cohesity cluster in the service provider's environment.
- **No need to open firewall ports**. Hybrid Extender eliminates the need for opening inbound ports on the firewall for the tenant.
- **Direct, unique connection to tenant vCenters**. It enables Cohesity to uniquely identify each tenant infrastructure entity (each tenant's vCenter server), even when using the same IP ranges.
- **Source-side deduplication**. Because the Hybrid Extender has a Cohesity agent running on it, it can perform source-side dedupe to reduce the actual data transferred over WAN.
- **gRPC**. Hybrid Extender uses the gRPC tunnel for communication between the tenant and Service Provider. gRPC is a modern open-source Remote procedure call (RPC) framework that connects services in and across data centers with pluggable support for load balancing, tracing, and authentication.
- Tenant Active directory communication and configuration will work via HyX V2.
- It provides a single endpoint for all the tenant services and communicates via the gRPC tunnel.
- Hybrid Extender uses the TLS certificate as a foundation for secure communication.
- Provides tenant network isolation without VLANs and VPNs.

## Hybrid Extender Load Balancing

Hybrid extender V2 provides load balancing by distributing the traffic to the multiple VIPs of the Cohesity cluster in a single tenant by having multiple Hybrid Extenders. This ensures that none of the HyX or the VIP will bear too much load and spread the traffic evenly to improve the responsiveness by improving the performance and reducing the latency. It can also leverage the external load balancer to distribute the traffic. Two different networking approaches can deploy as below:

**Hybrid Extender Internal load balancing**: It is the most straightforward deployment method of internal load balancing by using the multiple VIPs on the Cohesity cluster, which will be a part of the HyX config file containing the hostname of the Cohesity cluster. It will fetch all the IPs from the DNS and communicate over them. The hybrid extender config file has 4 random IPs of the node for communication.

Figure 10: Hybrid extender internal load balancing




**NOTE**: There is no global communication between individual hybrid extenders. Each Hybrid Extender selects the Cohesity cluster VIPs at random which can result in sub-optimal sharing of load at times.

**Hybrid Extender with the external load balancer**: HyX will be configured with the endpoints of the external load balancer, and then the load balancer will distribute the traffic to the Cohesity cluster. The hybrid extender will be configured with the configuration file, which has the hostname of the load balancer. HyX will query DNS to get the IP of the cluster for all the outbound communication. For example, the external load balancer will be configured with the four endpoints, and all the HyX will use the four IPs for communication by querying the DNS.

Figure 11: Hybrid Extender External Load balancer

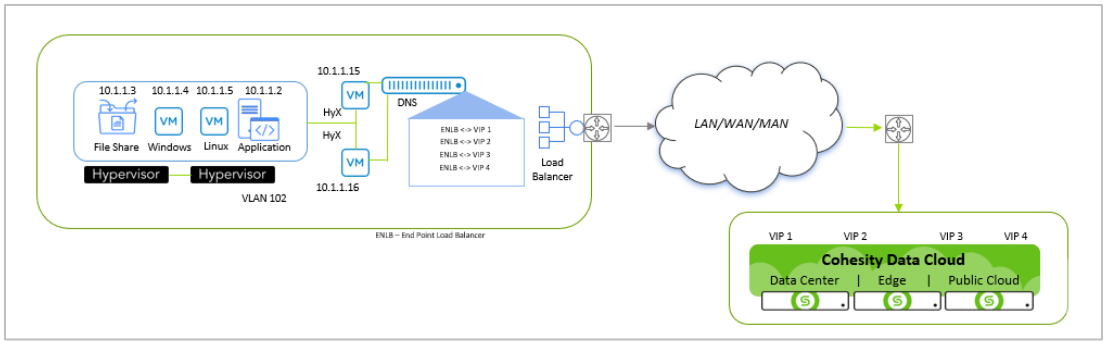
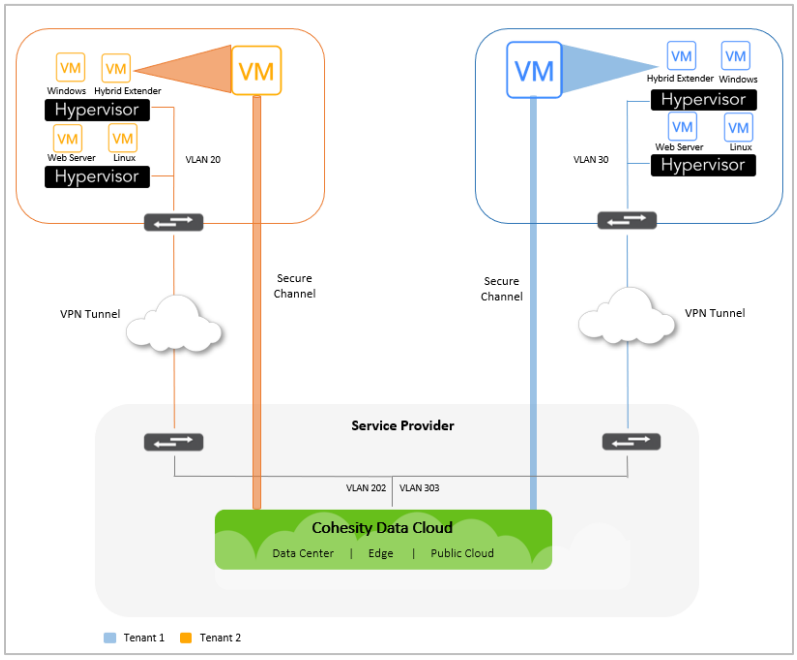



Figure 12 below illustrates how the Hybrid Extender establishes a secure channel for each tenant.

1. As the tenant administrator, you upload the configuration file to Hybrid Extender.
2. The Hybrid Extender initiates a connection to Cohesity Platform.
3. Cohesity communicates back at port 29991 and a secure channel is established.

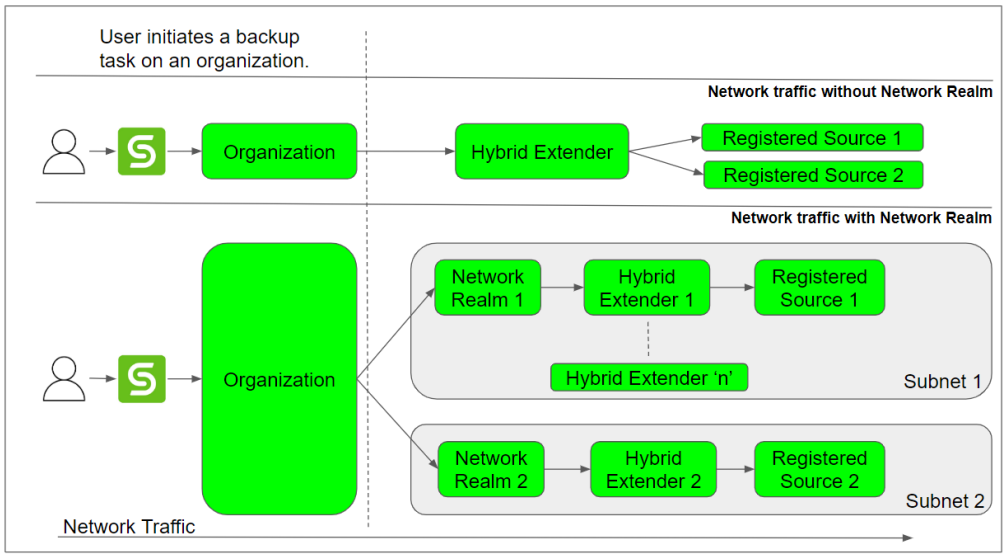
Figure 12: Secure Channel Setup Over Cross-Connect and VPN Tunnel Connections




## Network Realms for Multi-tenant Environments

Each Tenant can have multiple networks, one for production, one for testing and another for DMZ. To address this scenario, Cohesity introduces Network Realms for multi-tenant environments. Network Realm ensures source-level selection in a multi-tenant environment and allows you to create and manage multiple isolated networks within a tenant. On a Cohesity cluster, a source and a hybrid extender can be associated with a Network Realm to create an isolated network.

When a backup task is initiated on a Cohesity cluster, it reaches out to the Hybrid Extender associated with the Network Realm for the source IP address. You can associate the source with the Network Realm during its registration and each source can be associated with only one Network Realm. However, you can associate multiple Hybrid Extenders with a Network Realm. The Network Realm maintains the list of registered sources on a Cohesity cluster to create isolated networks. An isolated network ensures that a task on a Cohesity cluster doesn't fail due to a mismatch of IP addresses from multiple sources.



## Deploy the Hybrid Extender

When using the Hybrid Extender to back up data from a tenant's environment to Cohesity Platform, it is important to review which workload types are supported in different versions of the Cohesity Hybrid Extender. Hybrid Extender V2 supports the workflow as mentioned in Remote Backup: Supported Workloads.

To use the Hybrid Extender, you will:

1. Deploy the Hybrid Extender on the tenant's vCenter server.
2. As part of that process, you will upload a configuration file on the Hybrid Extender **Upload** page.

To deploy and configure the Hybrid Extender for a tenant account, confirm that the service provider has enabled it and then follow the tenant Hybrid Extender instructions below.

For information on Hybrid Extender sizing, see Appendix B and for upgrading the Hybrid Extender from Version V1 to V2, see Appendix F.

## Ports Used by Hybrid Extender

For more information about ports used by Hybrid Extender, see Hybrid Extender.



# Manage Organizations with Isolated Namespaces

In a Cohesity cluster that is configured for multiple tenant organizations, each tenant is implemented as an *organization*. The Organization ID acts as the multi-tenancy identifier for each tenant. Organizations act as namespaces to tie all the resources assigned to the organization. Some resources—such as Organization Users/Administrator, Views, VLANs, and Sources—are isolated per tenant, while other resources—such as Storage Domain and Protection Policies—can be dedicated or shared, depending upon the specific tenant and service provider requirements of the deployment.

## Tenant Organization Administration

Managing the tenant organization administration is a shared responsibility. There is a set of tasks and workflows that the service provider must implement, and there is a different set of tasks and workflows that the tenant administrator must implement. Therefore, there are two levels of administration:

- **Service Provider Administrator**: This role has the same overarching permissions to the system as the administrator on a non-multi-tenant Cohesity cluster.
- **Tenant Administrator**: This role manages the tasks that are specific to a tenant organization on a multi-tenant Cohesity cluster.

For more insight into the administrative scope for service provider administrator and tenant administrator, see Compare Service Provider and Tenant Administrator Privileges.

### Cohesity Organizations using Helios

Helios is a SaaS-based management platform that provides a single view and global management of all your Cohesity clusters, whether on-premises, cloud or Virtual Edition, regardless of the cluster size. You can quickly connect clusters to Helios and then access them from anywhere using an internet connection and your Cohesity Support Portal credentials.

Helios supports the multitenancy feature. The multitenancy feature enables you to configure the multitenant environment on Helios and securely isolate each tenant in your environment.

Service Providers can use Helios to manage tenants and tenant lifecycle across multiple clusters. Service Providers can isolate tenant services across multiple clusters. Helios provides a single pane view to service providers and tenants across multiple multi-tenant clusters.

### Supported Multitenancy Operations

- The SP administrator can:
  - Claim new clusters or add existing multi-tenant clusters
  - Create, read, update, and delete tenants, tenant users, and tenant groups
  - Assign one or more Cohesity clusters to an organization
  - Activate or deactivate organizations
  - Switch to an organization

- The tenant administrator can:
  - Monitor services through Helios dashboards
  - Add an Identity Provider (IdP) so that tenant users can log in to Helios using Single Sign-On (SSO)
  - Perform actionable search.

# Onboarding Workflow (Service Provider Administrators)

Service provider administrator has the responsibility to on-board the tenants by creating organizations and doing the required configuration. Here's a typical workflow a service provider administrator needs to execute per tenant. Throughout, for more details, see Organizations (Multitenancy).

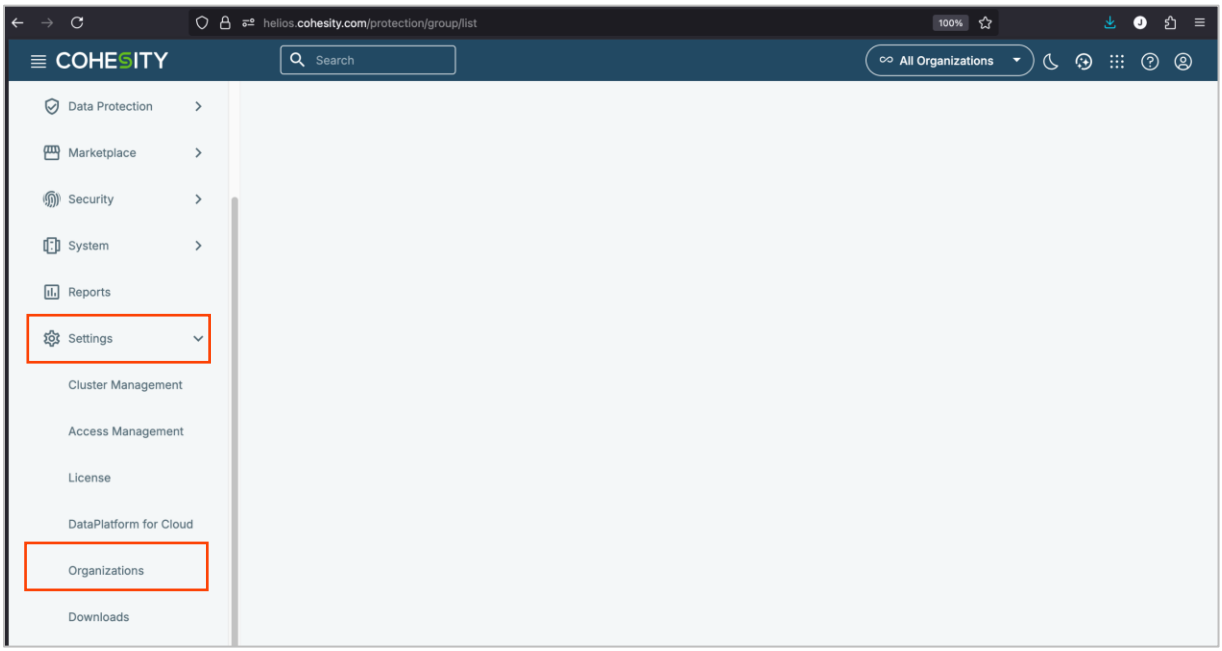
1. Enable Organizations
2. Add an Organization
3. Assign Systems
4. Add Service Provider User
5. Add Organization User
6. Assign Sources and Objects
7. Create Policies

## Enable Organizations – Helios Workflow

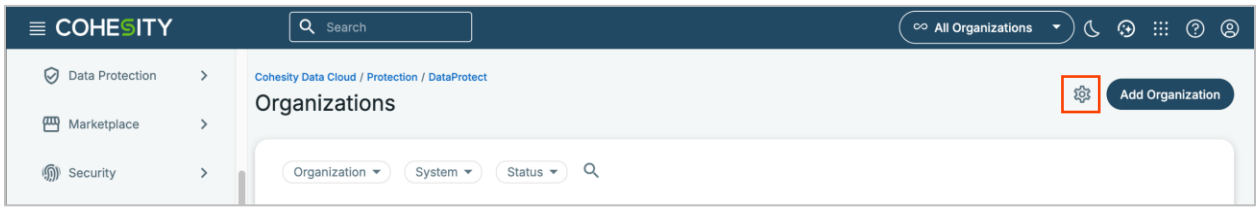
To use the **Organizations** feature and create organizations, you must enable organization management from Helios. After enabling the feature, you can add new organizations from the **Organizations** page.

To enable the **Organizations** feature:

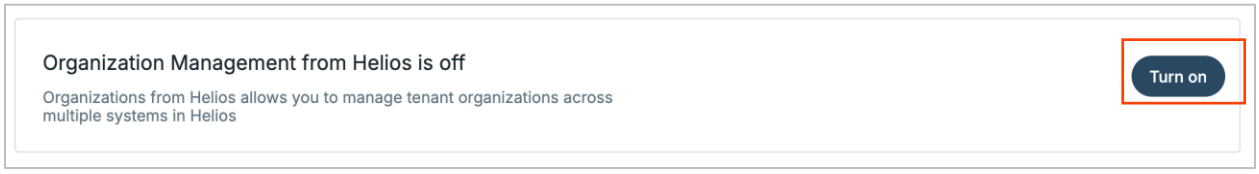
1. In Cohesity Helios, navigate to **Settings** > **Organizations**.



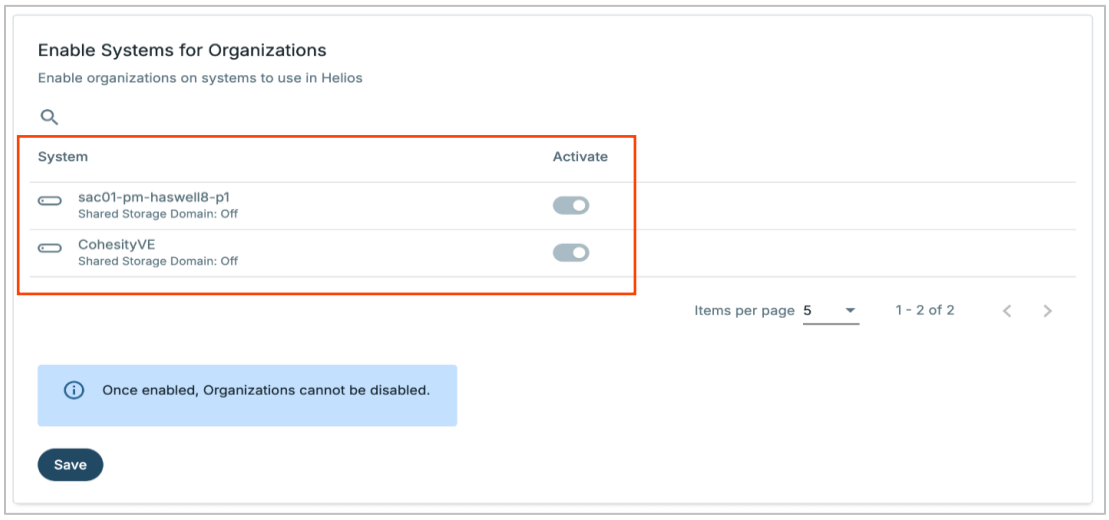
2. Click on settings gear icon.




3. Enable Organization Management from Helios, by clicking **Turn on**.




4. After you enable organization management, all the clusters registered with Helios are displayed in the **Enable Systems for Organizations** section:

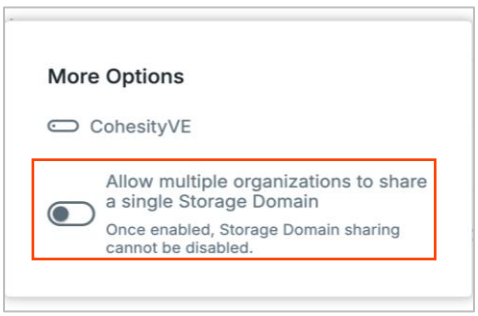



5. Turn on the toggle corresponding to the cluster to enable multitenancy on the cluster.

> **NOTE**: If you do not turn on the toggle, multitenancy is not enabled on the corresponding cluster.

Optionally, you can allow multiple organizations to use one storage domain. To allow multiple organizations to share one storage domain, hover over the cluster and click the toggle.

- On the More Options dialog, turn on the Allow multiple organizations to share a single Storage Domain toggle:




6. Click **Save.**

## Add an Organization

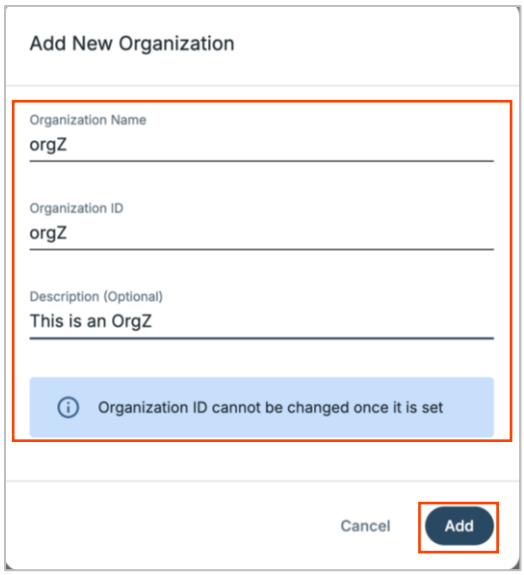
An organization must have a name and an organization ID.

To add an organization:

1. In Cohesity Helios, navigate to **Settings > Organizations.**
2. Click **Add Organization.** The **Add New Organization** dialog is displayed.
3. On the **Add New Organization** dialog:
   a. Enter a name for the organization. You can edit the name after adding the organization.
   b. Enter an ID for the organization. The ID can be up to ten alphanumeric characters.

   > **NOTE**: You cannot edit the organization ID. Even if the organization is deleted, the ID cannot be reused. Uses the same organization ID across clusters.

   c. Optionally, you can enter a description for the organization.
4. Click **Add**.




## Assign Systems

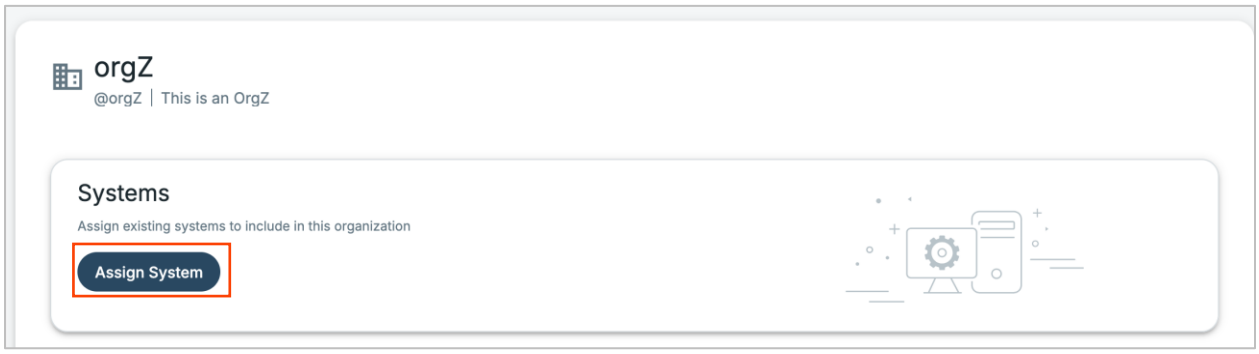
After you assign a cluster, you cannot remove it from the organization.

> **NOTE**: After you assign a cluster, you cannot remove it from the organization.

To assign clusters to this organization:

1. In DataProtect, navigate to **Settings** > **Organizations**.
2. On the Organizations page, click the organization name to drill down to the organization details page.

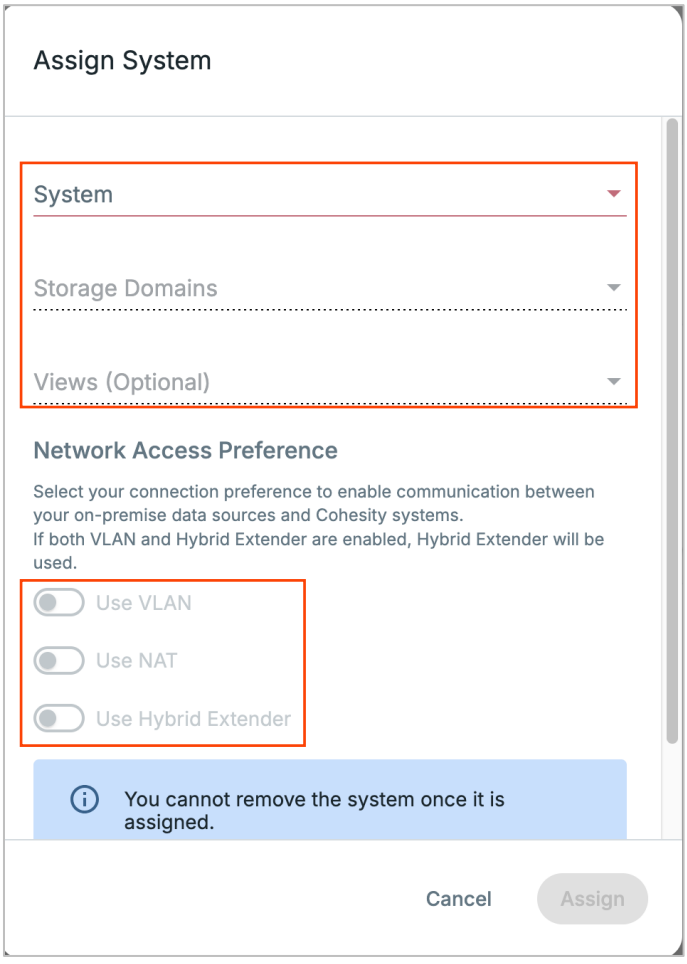
3. On the **Systems** section, click **Assign System**.




4. On the **Assign System** dialog, do the following:
   - Select a cluster from the **System** drop-down list.

     A cluster may show up as disabled if:

     - The cluster is disconnected from Helios.
     - The **Organizations** feature is not enabled on the cluster.
     - The cluster is running an unsupported version. The Cohesity cluster must be running 6.6.0c or a later version.
   - Select a storage domain from the **Storage Domains** drop-down list.
   - Optionally, you can select a view from the **Views** drop-down list.



5. On the **Network Access Preference** section, select the network preference:
   - Turn on the **Use VLAN** toggle to use VLANs to segregate traffic. For more information, see Assign VLANs.
   - Turn on the **Use NAT** toggle to set service provider side NAT. For more information, see Assign NAT IP Addresses.
   - Turn on the **Use Hybrid Extender** toggle to enable Hybrid Extender. For more information, see Enable and Deploy Hybrid Extender.
   - Communication between your on-premises data sources and Helios is routed through the network connection you select.
   - If you enable both VLAN and Hybrid Extender, Hybrid Extender connection uses VLAN.
5. Click **Assign**.

# Configure Network Settings for an Organization

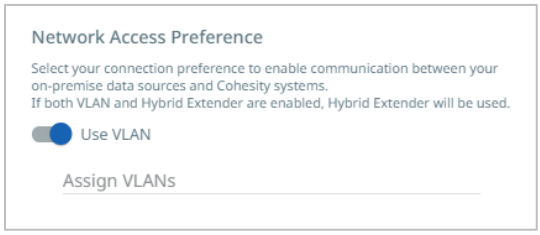
The network settings for an organization involve assigning VLANs (optional) and setting service provider side NAT.

## Assign VLANs

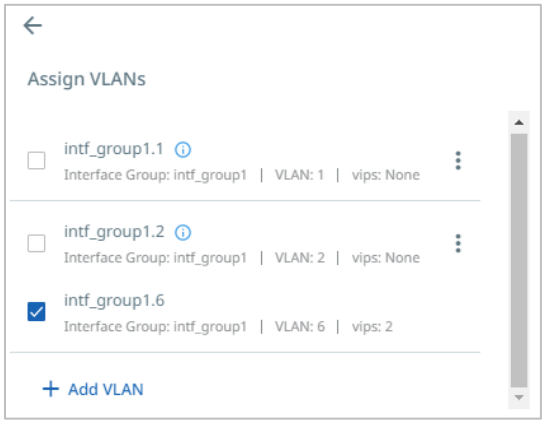
To isolate network traffic for the organization, assign VLAN IDs. VLANs can be added and removed later. Use VLANs to segregate traffic across different tenants. If you use VLANs, you must assign VLANs to tenants. Each tenant can be assigned a VLAN.

To assign VLANs:

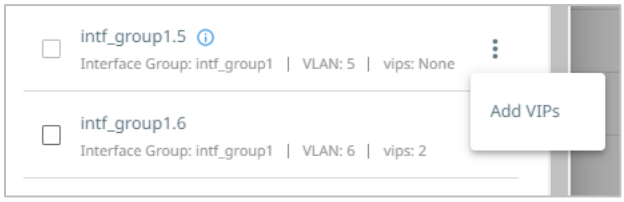
1. On the **Network Access Preference** section, turn on the **Use VLAN** toggle and click **Assign VLANs**.




2. On the **Assign VLANs** dialog, select an interface group(s) and click the back arrow.



3. Without VIPs, you cannot assign an interface group to an organization. To add VIPs, click ⋮ and click **Add VIPs** and enter the IP address and range:

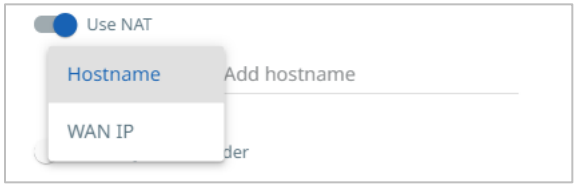



4. To add a new VLAN, click **Add VLAN** and do the following:
   a. Select an interface group from the **Interface Group** drop-down list.
   b. Enter a VLAN ID.
   c. Select the protocol: IPv4 or IPv6.
   d. Enter the subnet in a valid CIDR format.
   e. Enter the gateway IP address.
   f. Turn on the **Enable For All Organizations** toggle to ensure that the same network can be used for backing up different tenants' data.

## Assign NAT IP Addresses

To assign NAT IP addresses:

1. On the **Network Access Preference** section, turn on the **Use NAT** toggle.



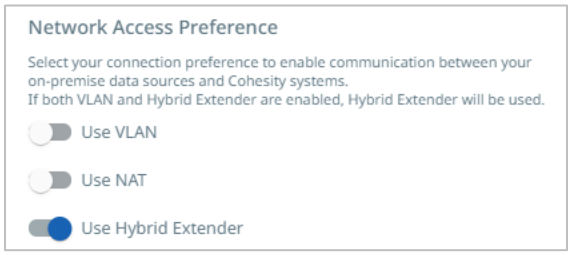

2. Select one of the following options:
   - **Hostname**—Specify the hostname.
   - **WAN IP**—Specify public IP addresses so that the organization can use these entries to reach out to Cohesity nodes.

# Enable and Deploy Hybrid Extender

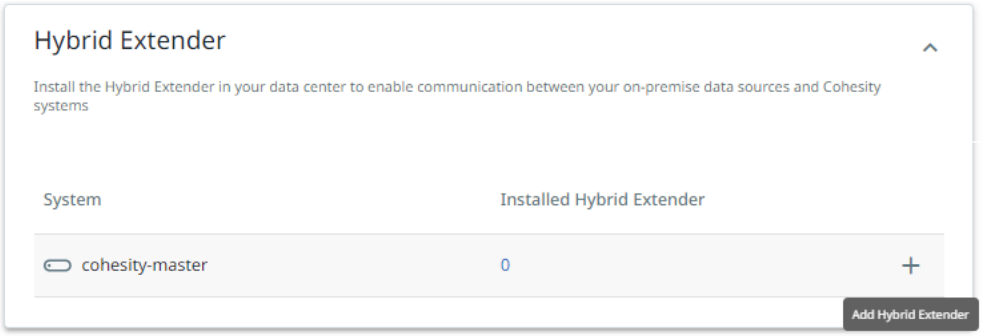
As a service provider, if you are serving multiple organizations in isolated networks with the same IP address ranges and subnets on Helios, you may need to enable the Hybrid Extender. Once the service provider administrator or Helios administrator enables Hybrid Extender, the organization administrator can deploy and configure the Hybrid Extender.

To enable Hybrid Extender:

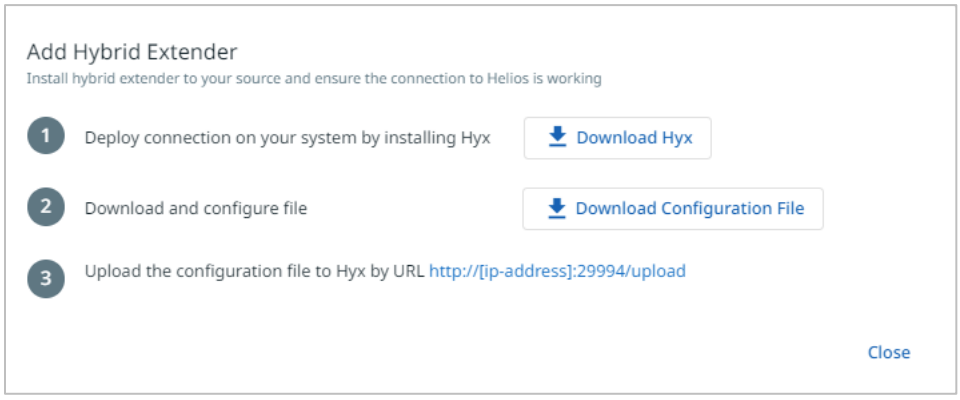
1. On the **Network Access Preference** section, turn on the **Use Hybrid Extender** toggle.




2. Click **Assign** to assign the cluster to the organization.
3. On the **Hybrid Extender** section, click the dropdown and click **+** to add the Hybrid Extender.




4. Install the Hybrid Extender in your data center to enable communication between your on-premises data sources and Helios.




For more information about Hybrid Extender, see Cohesity Platform documentation.

## Add Service Provider User

A service provider administrator is typically a user with the default administrator role. Technically, the service provider administrator is the same as the Helios administrator. In the context of the **Organizations** feature, the service provider administrator manages multiple organizations. The service provider user can be:

1. A Helios user
2. An SSO user
3. An SSO group

For more information about adding user(s) as a service provider user, see Cohesity Access Management Documentation.

## Add Organization User

The organization user must be an SSO user or an SSO group and can access only the corresponding organization. An organization user with the administrator privilege is called the organization administrator and users without the administrator privilege are called organization users.

- **Organization Administrator**—An organization administrator can manage their organization in a multitenant environment. The organization administrator role and its privileges are defined by the service provider administrator. The organization administrator can create an organization user or group. However, the organization administrator cannot create or modify roles.
- **Organization Users**—An organization user or group is created by the organization administrator or it can be assigned to the organization by a service provider administrator. The organization administrator can only assign the inherited roles to a new organization user or group. The roles can be Viewer, Operator, or other custom roles.

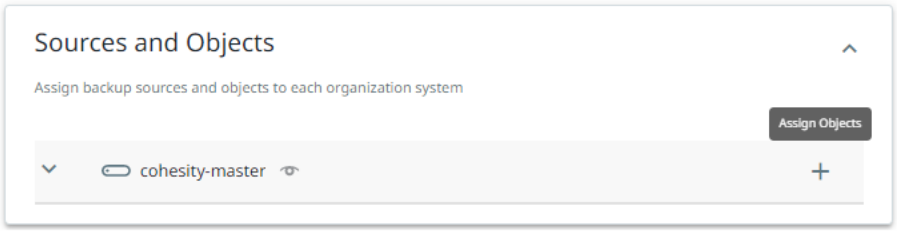
For more information about adding user(s) as a Organization user, see Cohesity Access Management Documentation.

## Assign Sources and Objects

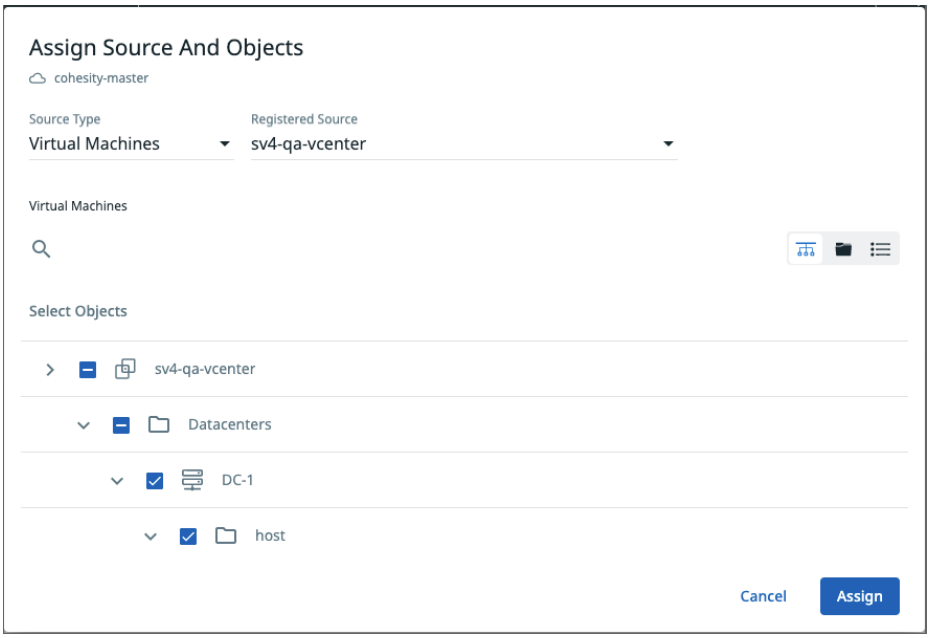
You must assign sources and objects to each cluster belonging to the organization.

To assign sources and objects:

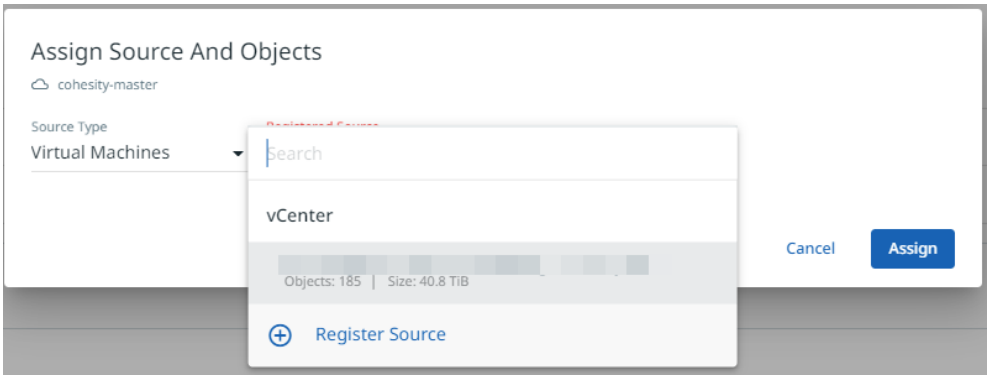
1. In **Cohesity Helios**, navigate to **Settings** > **Organizations**.
2. On the **Organizations** page, click the organization name to drill down to the organization details page.
3. On the **Sources and Objects** section, click the drop-down to view the clusters assigned to the organization and click **+** to assign objects.



4. On the **Assign Sources** and **Objects** dialog:
   - Select the source type from the **Source Type** drop-down list and select the source from the **Registered Source** drop-down list.
   - Select the objects and click **Assign**.




**NOTE**: You can also register a new source. From the Registered Source drop-down list, click **Register Source**.




For more information about the procedure to register sources, see Cohesity Data Cloud (Self-managed) documentation.

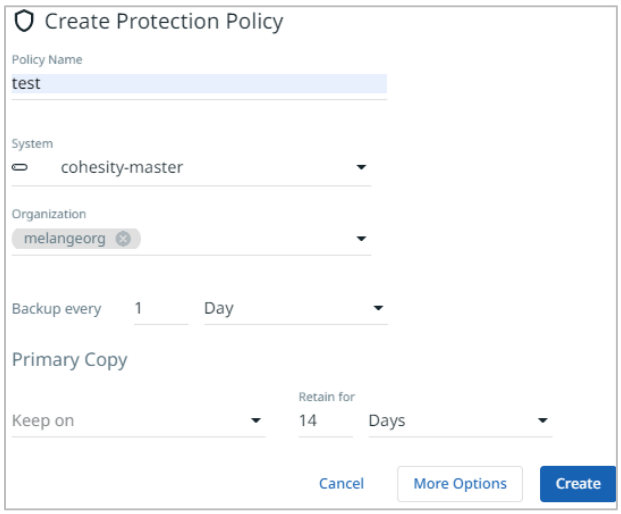
## Create Policies

A policy is a reusable set of settings that define how and when objects are protected, replicated, or archived. You can select which policy to use when configuring a Protection Group. A Protection Group uses the schedules and settings defined in the policy to determine when and how backups are captured, archived, or replicated.

The service provider administrator must create a policy and assign it to the organization. Organization users cannot create policies.

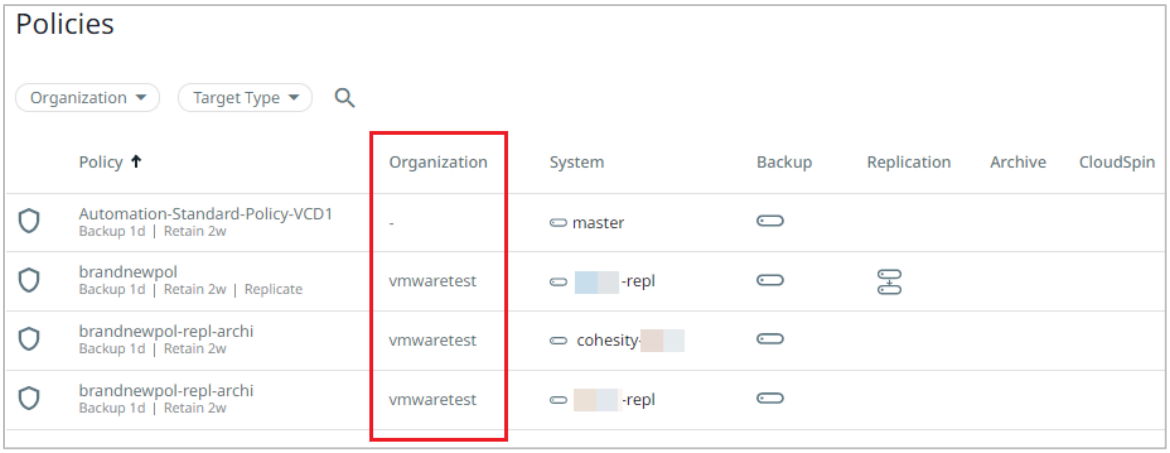
To create a policy and assign it to an organization:

1. In DataProtect, navigate to **Data Protection** > **Policies**.
2. Click Create Policy.




3. On the Create Protection Policy dialog:
   - Enter a policy name.
   - Select the cluster belonging to the organization from the **System** drop-down list.
   - Select the organization from the **Organization** drop-down list.
   - Configure other parameters as necessary. For more information, see Cohesity Data Cloud (Self-managed) documentation.
   - Click **Create**.

The policy is created, and the organization can use this policy. The policy is listed on the **Policies** page.

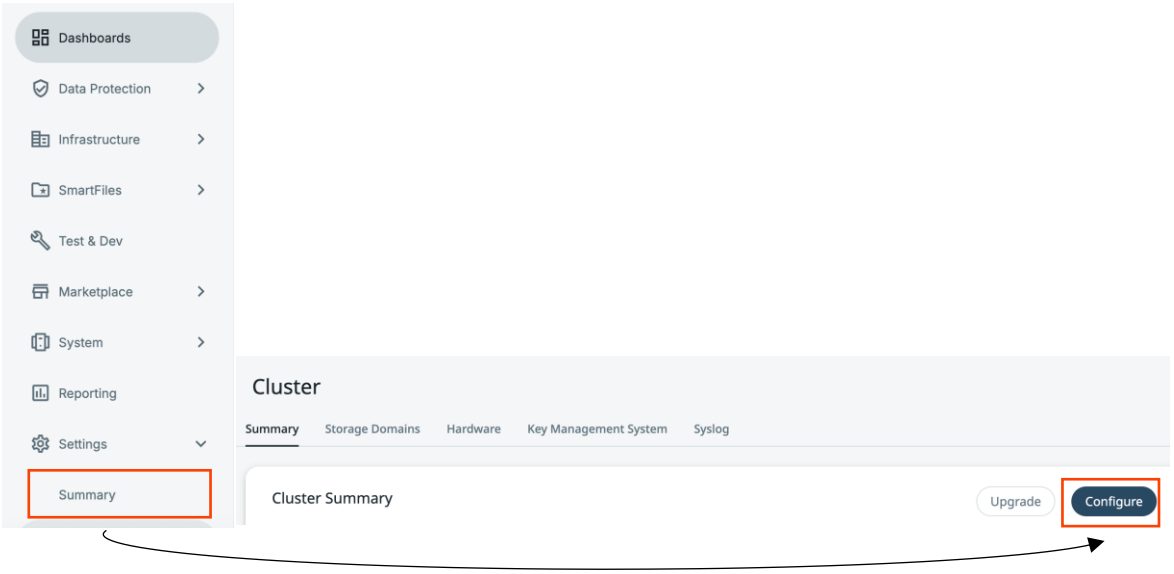



**NOTE**: The policy is listed in the **Policy** drop-down list when the organization administrator creates a new protection group.

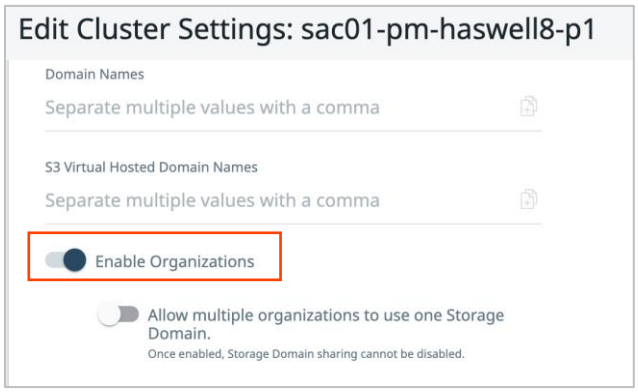
## Enable Organizations – Cluster UI Workflow

If the Clusters are not connected to Helios, to use the **Organizations** feature and create organizations, you must enable organization management from Cohesity Data Cloud Cluster UI.

1. Log in to Cohesity Data Cloud UI as Service Provider administrator and select **Settings > Summary** and click **Configure**.



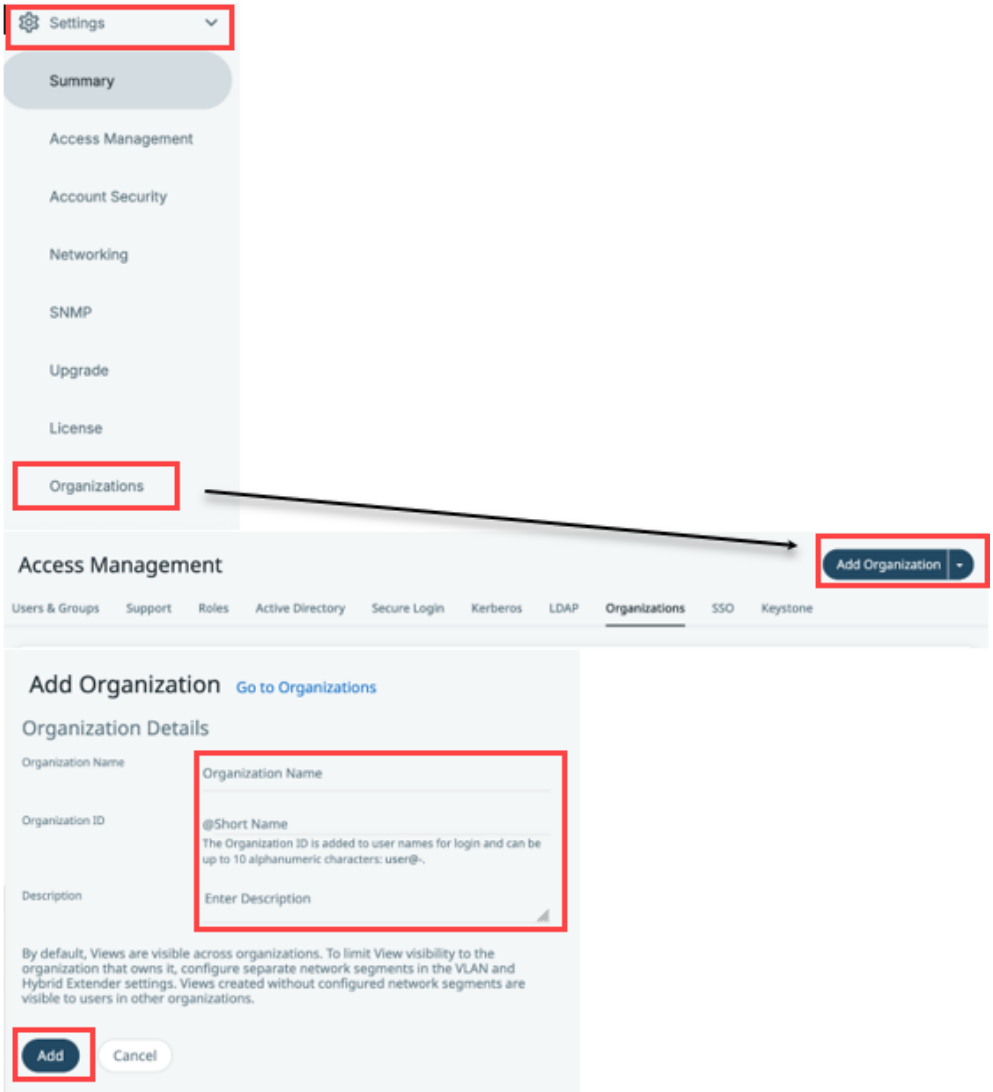
2. In the **Edit Cluster** settings, turn on **Enable organizations** and click **Save**.




Once enabled, service provider administrators can create organizations for the tenants they wish to onboard. Repeat the same steps for other clusters on which Cohesity Organizations must be enabled.

## Add an Organization – Cohesity Cluster

1. Create **Organizations**. Navigate to **Settings** > **Organizations** and click **Add Organization**.



2. In the form that opens:

   a. Enter the Organization Name and Organization ID and Description. Click Add.

   > **NOTE**:
   >
   > The Organization ID is a short string (to be used for logins in the form of <User>@<Organization_ID>) that can include no more than 8 alphanumeric characters and must be unique in the system.
   >
   > The Organization ID cannot be edited later. If the organization is deleted, the Organization ID cannot be reused.

   b. **Create and assign Storage Domains**: Assign Storage Domains and Views. The service provider administrator can choose to create a dedicated storage domain per tenant or share a storage domain across multiple tenants.

   c. **Assign and Join Active Directory/LDAP/Keystone**: Assign the already configured ADs/LDAP/Keystone or add the new AD/LDAP/Keystone to the tenant.

   > **NOTE**: You cannot assign an AD/LDAP/Keystone on a parent/root level to multiple tenants or service providers and tenants. Instead, it's advisable to add the AD on the root level to the Service provider and group to the tenant.

   d. **Create a tenant organization administrator**. The service provider administrator must create and assign a tenant administrator user and group for tenant self-service. For instructions, see Organizations (Multitenancy).

   e. **Assign Objects from Registered sources**. An object can be assigned from the register source to the tenant, and it will be part of the specific tenant.

   Table 4: Sources and Tenants

| Source | Components |
|---|---|
| VMware vCenter | • Entire VC<br>• VMware DC<br>• ESXi cluster<br>• ESXi host<br>• Folders<br>• Resource pools<br>• VMs |

   > **NOTE**: You cannot assign the same source to two different tenants. Example: You can't add the same VCenter. Instead, you can add VCenter to the Cluster source or service provider and add its component to another tenant.



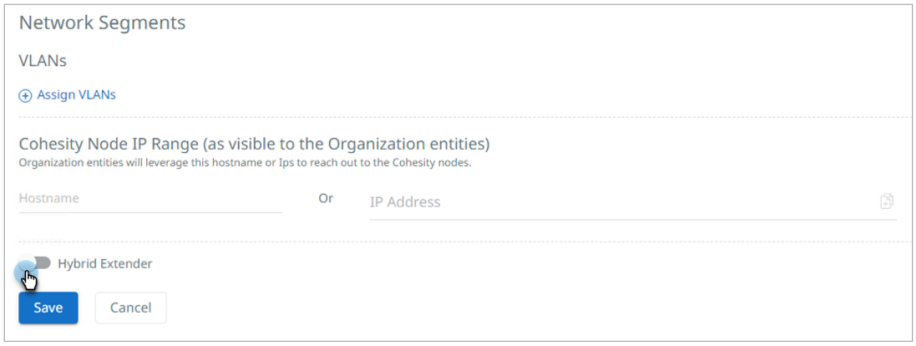
f. **Create and assign Protection Policies**. The service provider administrator needs to create and configure Protection Policies for their tenant organizations and then assign them to each tenant organization.

> **NOTE**: New clusters include three default Protection Policies: *Bronze* (daily backup, 30-day retention), *Silver* (backup every 6 hours, 7-day retention), and *Gold* (hourly backup, 2-day retention). If these meet your tenants' needs, you do not need to create additional Protection Policies.

g. **Assign VLANs**. To achieve network isolation between tenants, create and assign VLANs to each tenant. For instructions, see Organizations (Multitenancy).

> **NOTE**: From Version 6.4 and higher, service providers can create a VLAN that can be shared across tenants using the **Enable for all Organizations** option while creating a VLAN.

h. **Enable Hybrid Extender for tenants**. If you host multiple customers with the same IP address ranges and subnets on the same Cohesity cluster, enable **Hybrid Extender**.




Once enabled by the service provider administrator, the tenant administrator will be able to deploy and configure Hybrid Extender.

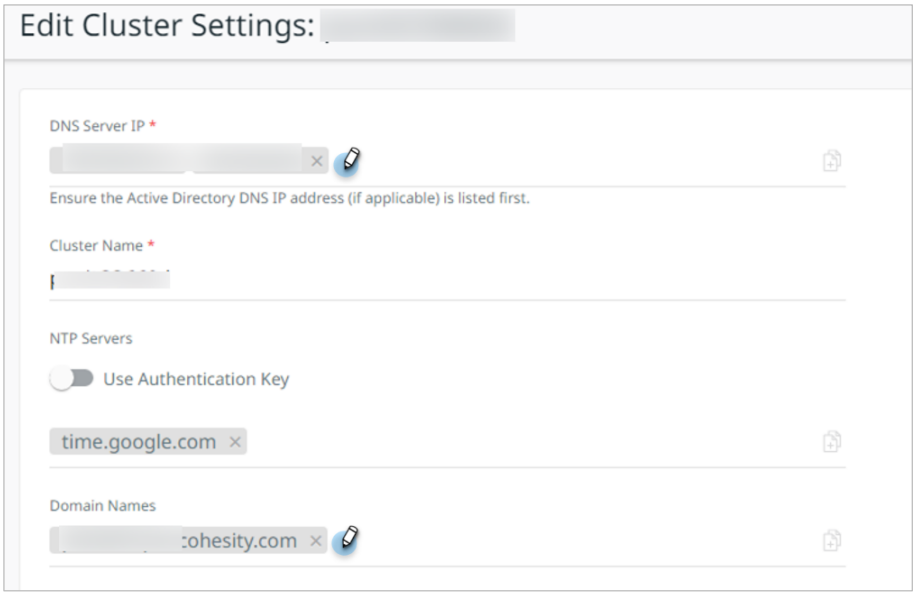
3. **Allowlist IPs on Cohesity Platform**. For VPN tunnel-based networks, ensure that the public NAT IP address of the organization's private network is added to the Global Allowlist. For instructions, see Add Subnets to Allowlists in the online Help.

4. **Add the tenant DNS and Domain Name to the Cohesity cluster**. Add the tenant organization's **DNS Server IP** and **Domain Names** to the Cohesity cluster.

   a. Navigate to **Settings** > **Summary**.

   b. On the Summary page, click **Configure**.

   c. Enter the DNS Server IP and Domain Names, then click **Save**.




5. **Create stub zones for tenants**. Organizations own their own Active Directory (AD) zones. When business partners need to resolve data at a partner's organization, they use stub zones.

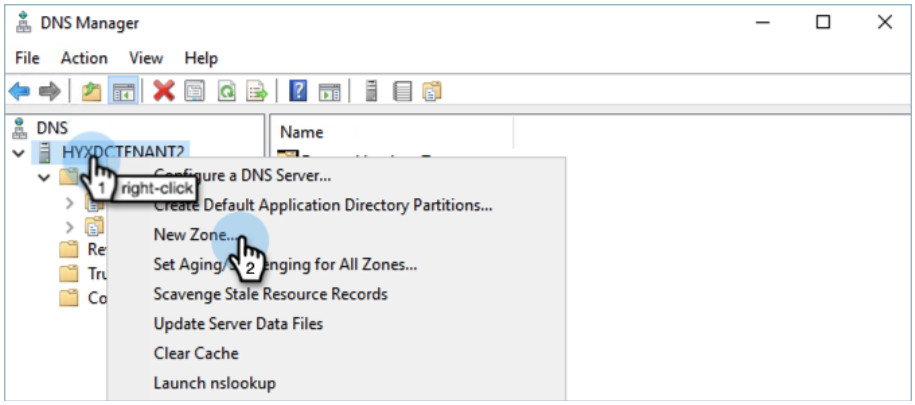
   As a behavior, the Cohesity cluster can only contact the first DNS server configured under the cluster settings. The first entry generally is for the service provider's DNS server. Therefore, the service provider's DNS must have stub zones configured for the other domains to reach any domain apart from its own.

   For tenant organization administrators to set up RBAC for their AD users, the service provider administrator must first create a stub zone on their DNS for each tenant domain.

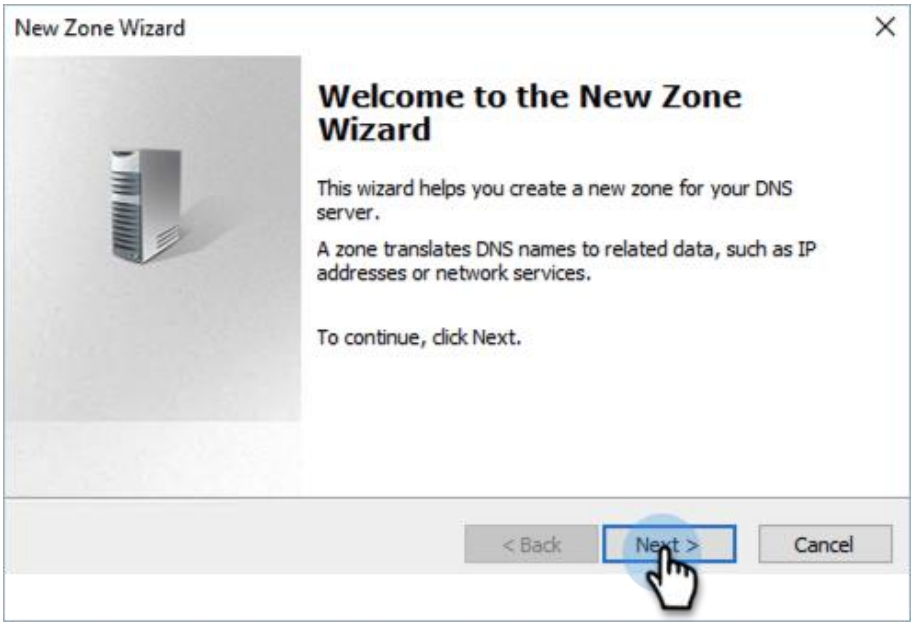
   To create a stub zone:

   a. Open the DNS Server Manager.

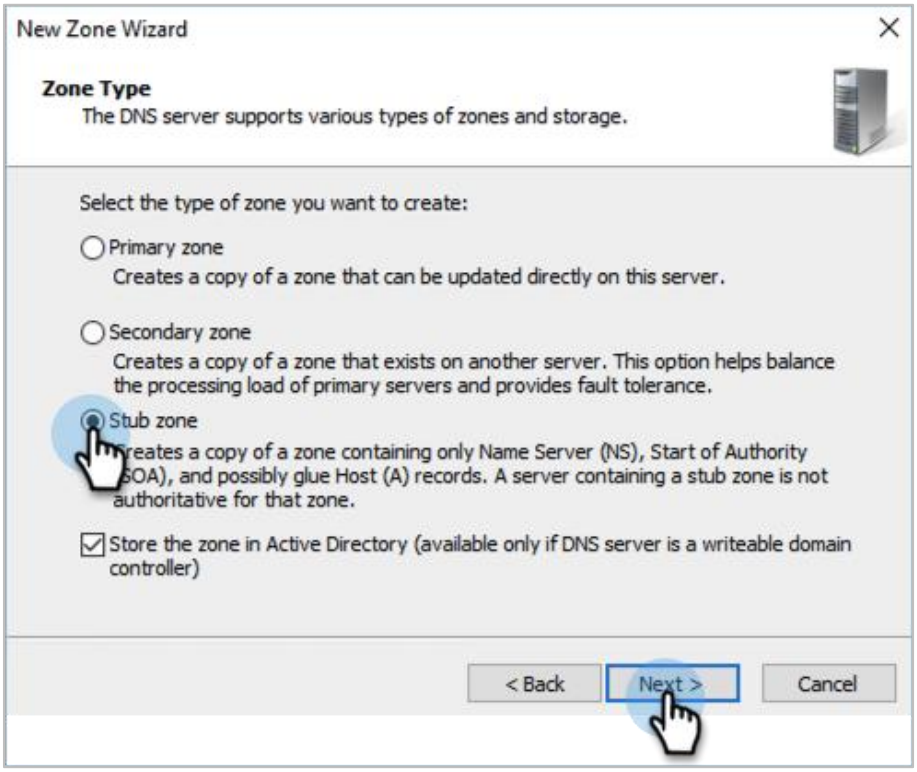
   b. Right-click the DNS server name and select **New Zone…**.



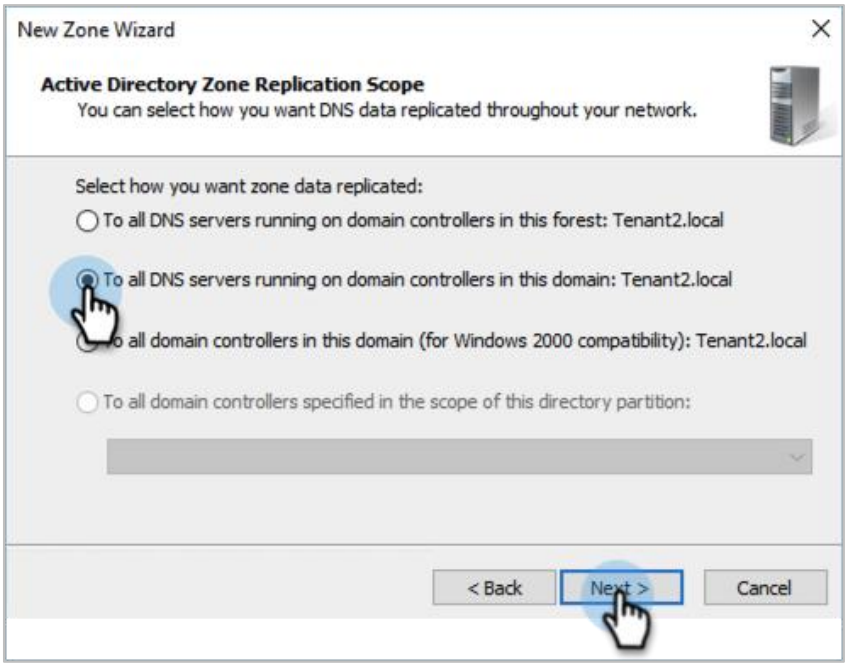
c. Follow the New Zone Wizard.



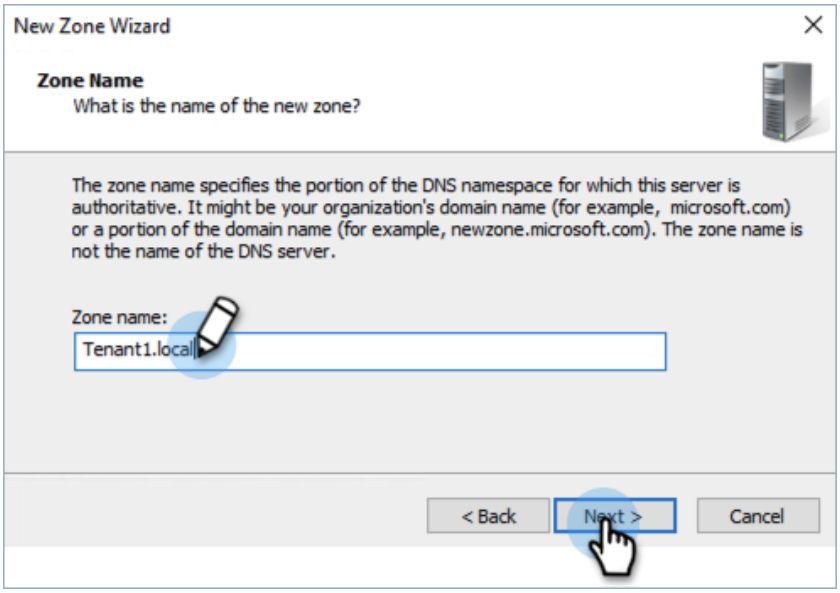

d. Under **Zone Type**, select **Stub zone**.



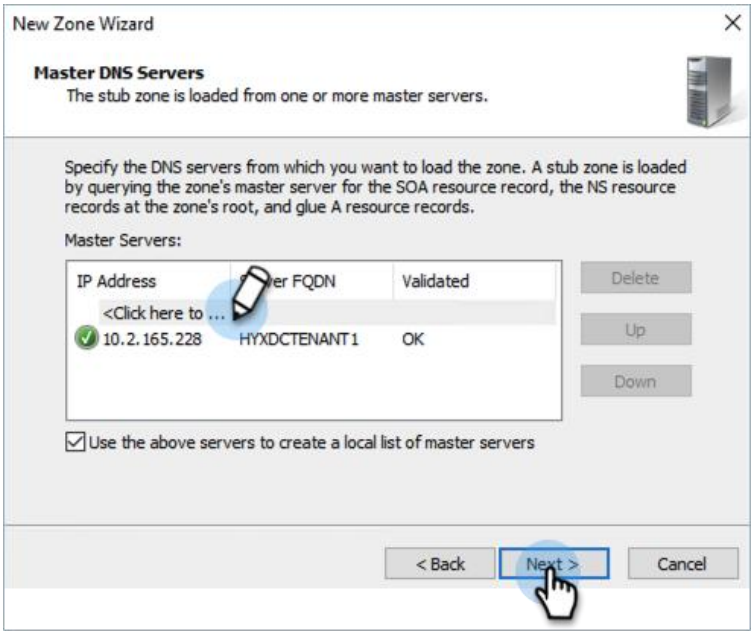
e. Under **Active Directory Zone Replication Scope**, select **To all DNS servers running on domain controllers in this domain**.




f. Enter the **Zone Name**.



g. Under **Master DNS Servers**, enter the **IP Address** for the domain for which you wish to create a stub zone.




h. Click **Finish** to close the wizard and create the new stub zone.


6. **Open ports for Active Directory**. To enable Active Directory communications with the Cohesity cluster.

Table 5: TCP ports required for Active Directory communication

| Port | Source | Target | Direction (from source) | Network Protocol | Usage Notes | Type of Traffic |
|---|---|---|---|---|---|---|
| 53 | Cohesity | DNS | Outgoing | TCP/UDP | DNS, if an external DNS server is configured. | Management |
| 88 | Cohesity | Kerberos Key Distribution Center (AD) | Outgoing | TCP/UDP | Required for Keberos if the cluster is configured to use Active Directory. | Management |
| 137 | Cohesity | Active Directory | Outgoing | TCP | Required only when initially joining the cluster to Active Directory. | Management |
| 139 | Cohesity | Active Directory | Outgoing | TCP | Required only when initially joining the cluster to Active Directory (for the NetBIOS session service). | Management |
| 389 | LDAP | Cohesity cluster | Outgoing | TCP/UDP | Required if the cluster is configured to use Active Directory or LDAP. | Management |
| 445 | SMB Clients | Cohesity SMB target | Incoming | TCP | SMB filer functionality. SMB and SMB2 restore. | Data Access |
| | Cohesity cluster | Active Directory | Outgoing | TCP | Required only when initially joining the cluster to Active Directory. | Management |

For updates, see Manage Firewall Ports.



## Configure a Tenant Organization

The tenant organization administrator is responsible for managing their organization. Once the service provider has created and configured your tenant organization, you, the tenant administrator, need to set up the initial configuration for your organization. For more details and configuration steps, see Organizations (Multitenancy).

To set up your tenant organization:

1. **Assign Sources**. Tenant administrators can add many different types of sources to the Cohesity cluster. For a list of supported workloads and workflows, see Supported Multi-Tenancy Workflows in the online Help.
2. **Add Protection Groups**. Tenant administrators can create their own Protection Groups and select which objects to protect in each. However, tenant organizations cannot edit the Protection Policies provided to them by the service provider.
3. **Configure role-based access control (RBAC) for tenant users**. Tenants can configure user roles for different user profiles with different privileges by using a combination of user roles and Active Directory/LDAP integration. Active Directory/LDAP integration allows the tenant administrator to assign specific roles for accessing Cohesity to Active Directory users within their organization.

   While service providers can create custom roles and assign them to tenant organizations, the roles for tenant users that a tenant administrator can manage include:

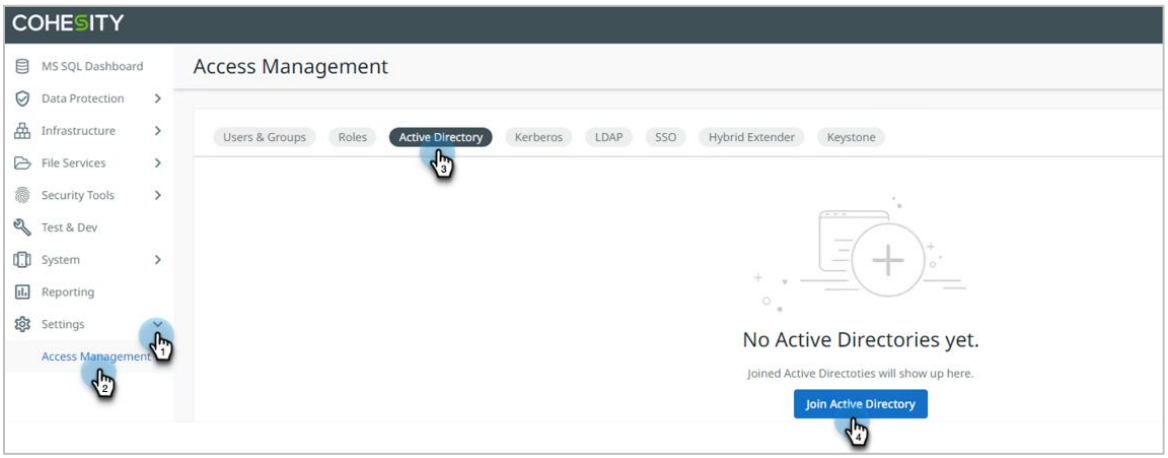
   Table 6: Tenant User Roles

| Role | Description |
|---|---|
| Admin | Tenant users who are assigned the Admin role have full access to all actions and workflows within their organization. For example, a user assigned the Admin role can create backups, recover snapshots and files from backups, and add sources. The Admin role can also add and delete users. |
| Operator | Users assigned the Operator role have Viewer role privileges and can run existing Protection Groups and create Recovery tasks. |
| Viewer | Users assigned the Viewer role have read-only access for all workflows within the Cohesity UI. |
| Self Service Data Protection | Users assigned this role have Viewer role privileges and can manage Clones and Protection Groups and Policies and can create Recovery tasks. |
| Data Security | Users assigned the Data Security role have Viewer role privileges and can create DataLock Views and set DataLock expiration dates. |
| Replication | User assigned the Replication role have access to set up and replicate data to another cluster. |
| SMB Security | User assigned the SMB Security Role has privileges to create, delete, and edit the SMB. |
| SMB Backup Operator | User assigned the SMB backup Operator role has the privilege to perform SMB backup, and SMB restore. |

**NOTE**: Before a tenant administrator can use Active Directory for RBAC, confirm that the service provider administrator has added the tenant DNS Server IP and Domain Names to the Cohesity cluster and created a stub zone on their DNS for tenant DNS domains.

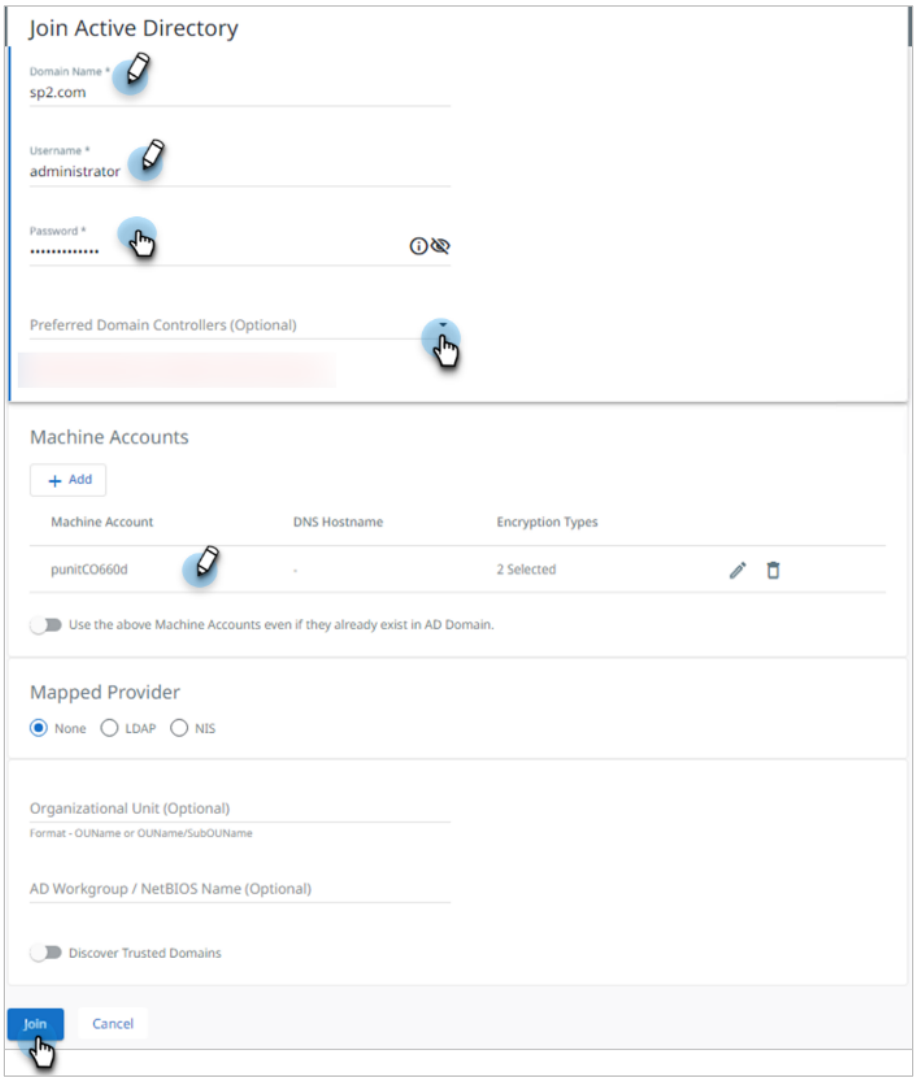
**To configure RBAC for a tenant's Active Directory users**:

1. Log in to a tenant organization with the tenant's admin role.
2. Go to **Settings** > **Access Management**. Click **Active Directory**> **Join Active Directory**.

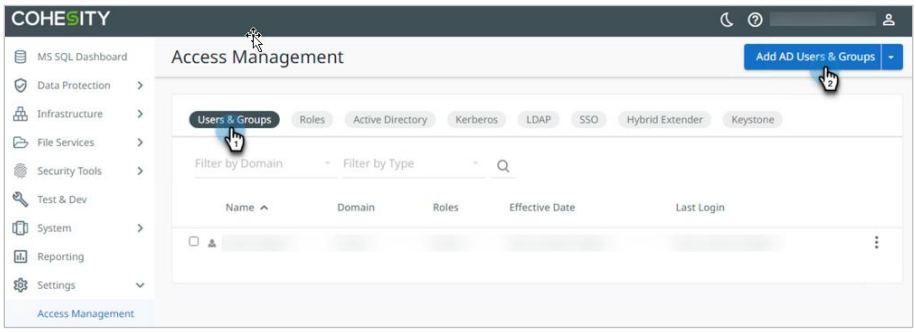



**NOTE**: Check your network connections to ensure that the tenant's DNS and Domain Controller are reachable from the Cohesity cluster.

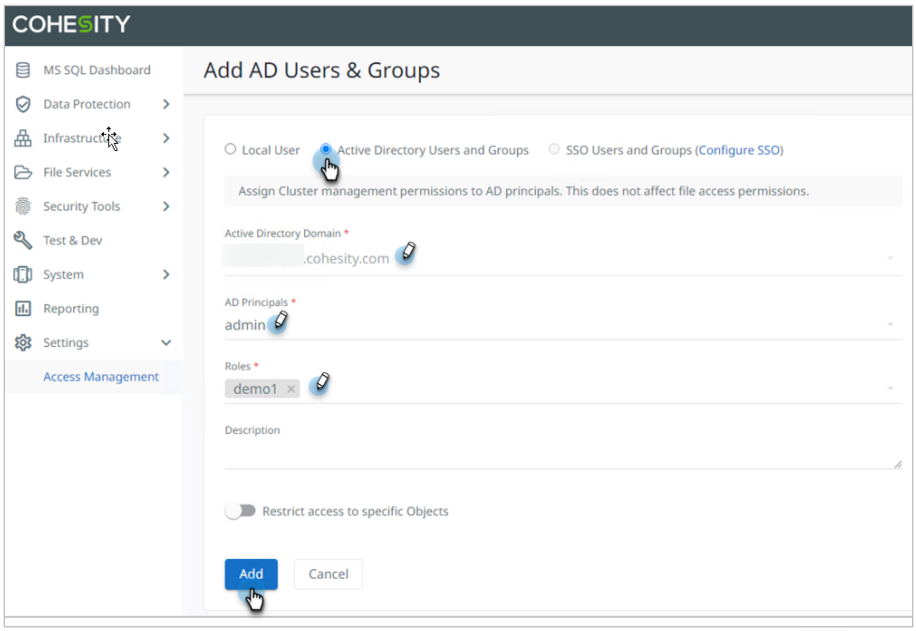
3. Enter the **Domain Name**, enter the AD admin account's Username and Password, select the **Preferred Domain Controllers**, assign names for the **Machine Accounts** and (according to your organization's naming convention), and assign names for **AD Workgroup/NetBIOS Name** and **Machine Accounts**. Click **Join**.




4. To add an Active Directory user to the tenant**,** select the **Users & Groups** tab and click **Add AD Users & Groups**.



5. Select **Active Directory Users and Groups**. Under **AD Principals,** search for the user or group to be added, select the appropriate **Roles** to assign, and then click **Add**.




> **NOTE**: Service providers can assign the same or different AD groups to multiple organizations. In that case, the user (in those AD groups) will have to specify ***<User>@<Organization_ID>*** under **Username** to log in.

6. Back on the **Access Management** page, under **Users & Groups**, you will now see the user you just added, with the role you assigned.

> **NOTE**: You can also use a SAML 2.0-based identity provider to configure SSO for the service provider and tenant organizations on the service provider's cluster.

7. **Deploy and configure the Hybrid Extender**. Cohesity has introduced the Hybrid Extender V2 from version 6.6 to enable service providers to host multiple customers with the same IP address ranges and subnets on the same Cohesity cluster. Following are the minimum requirements to deploy the hybrid extender.

Table 7: Deploy and configure the Hybrid Extender

| COMPONENT | REQUIREMENT |
|---|---|
| Memory | 4 GB RAM |
| CPU | 4 vCPU |
| Network Adapter | VMXNET3 |
| Space Requirement (Thick Provision Lazy Zeroed) | 74GB |

- Before you deploy the Hybrid Extender, open the following outgoing ports in the tenant's firewall and enable the Hybrid Extender for the tenant organization:

  Table 8: Firewall Ports

| PORT | SOURCE | TARGET | DIRECTION (FROM SOURCE) | NETWORK PROTOCOL | USAGE NOTES | TYPE OF TRAFFIC |
|---|---|---|---|---|---|---|
| 11117 | Hybrid Extender VM | Cohesity cluster | Outbound | TCP | Secure gRPC connections on cluster from Hybrid Extender VM. | Data path used to write data to Cohesity |
| 29991 | Hybrid Extender VM | Cohesity cluster | Outbound | TCP | Used in a multi-tenant environment for interaction between the Hybrid Extender and Cohesity cluster. | Control path |
| 29994 | Tenant Network | Hybrid Extender VM | Inbound | TCP | For uploading the config file for Hybrid Extender | Management |

  For updates, see Manage Firewall Ports in the online Help.

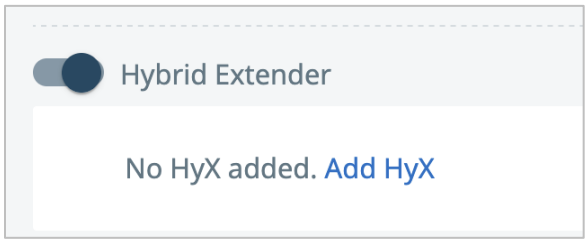
  **NOTE**: For the Hybrid Extender to communicate to the Cohesity cluster, only outgoing ports need to be opened on the tenant's firewall. You don't need to open any incoming ports.

- DNS configuration—The DNS configuration helps to look up the domain controller to join the Cohesity cluster to the tenant AD. This is used during source registration for name resolution and mount-based restores/clones for data protection of MS-SQL server, Oracle, etc.

  The following are the considerations for DNS configuration on Hybrid Extender:

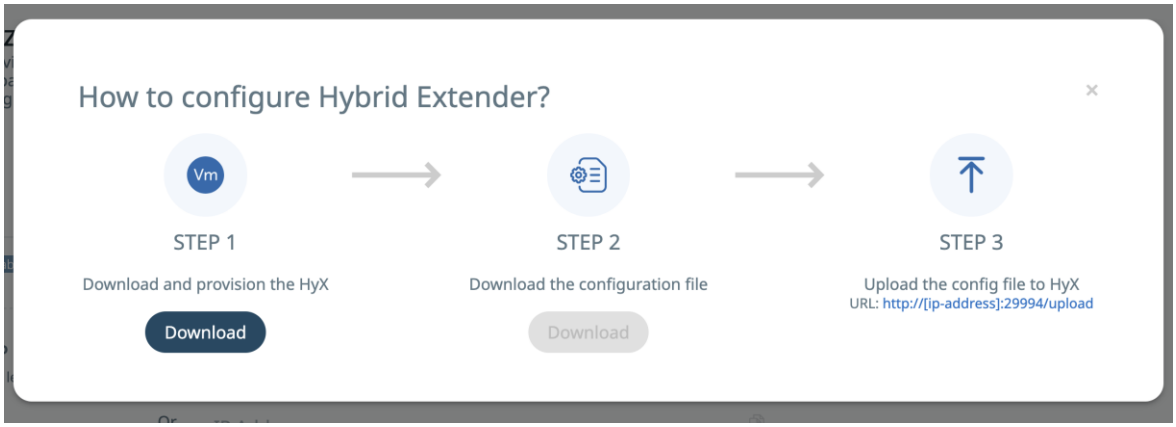
  - The Hybrid Extender automatically gets the DNS configuration when assigning an IP address using DHCP.
  - When you assign a static IP address, you must add the DNS in the Hybrid Extender VM by updating /etc/resolv.conf file. For any assistance, you may contact the Cohesity Technical Support team.
  - Network Time Protocol (NTP) has to be set up on the hybrid Extender to avoid the following:
    - RPC requests between the Hybrid Extender and the cluster can be timeout.
    - Time skew is more than 5 min between the AD server and the Hybrid Extender, Kerberos authentication may fail.

Post enabling the Hybrid Extender for the organization:

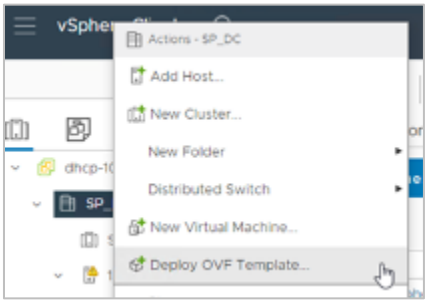



Click on **Add HyX** for step by step Instructions to deploy HyX and help with the configuration settings.

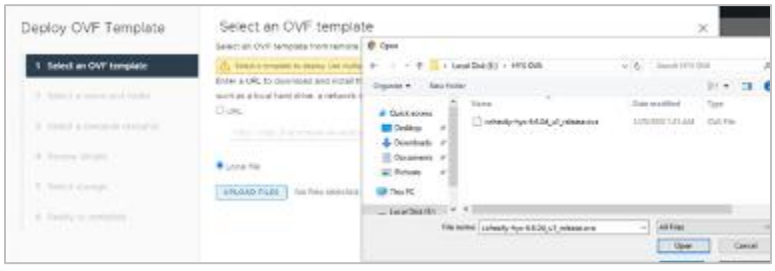
7. Download and provision the HyX. Click **Download** and provide the Cohesity login credentials, and ova download will start.




8. Deploy the Hybrid Extender OVA/OVF in the tenant infrastructure.
   a. Login to the VCenter and right-click on Datacenter.
   b. Select the option **Deploy OVF Template**.




9. Select the "Local file" on the **Select an OVF template** window and open the Downloaded OVA and Click **Open.**



10. Once the Hybrid Extender OVA is uploaded, then click **NEXT**.

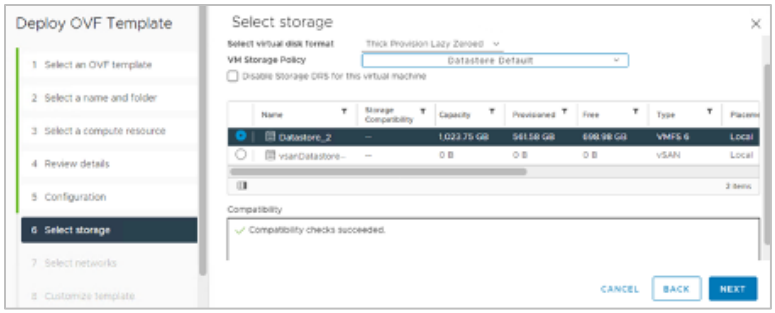

11. Enter the name of the Hybrid Extender Virtual Machine and select the Target location. Click **NEXT**.


12. Select the Destination Compute resource and click **NEXT**.

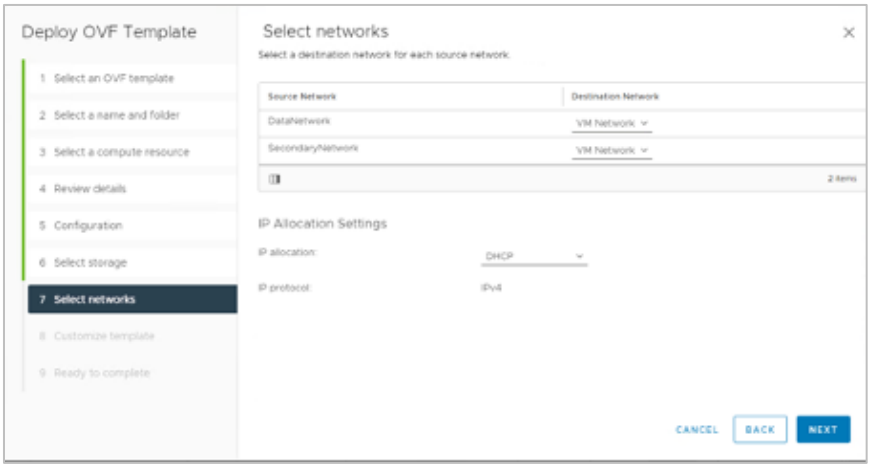

13. Review the Hybrid extender details and Click **NEXT**.

14. Select the Deployment configuration for Hybrid Extender and click **NEXT**.

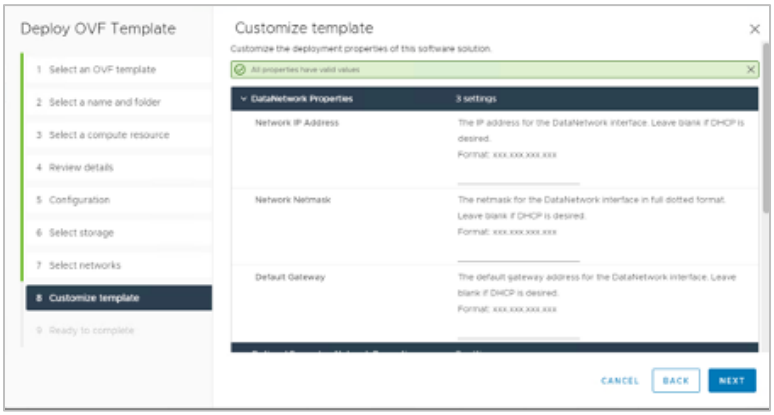

15. Select the compatible storage and datastore. Click **NEXT**.



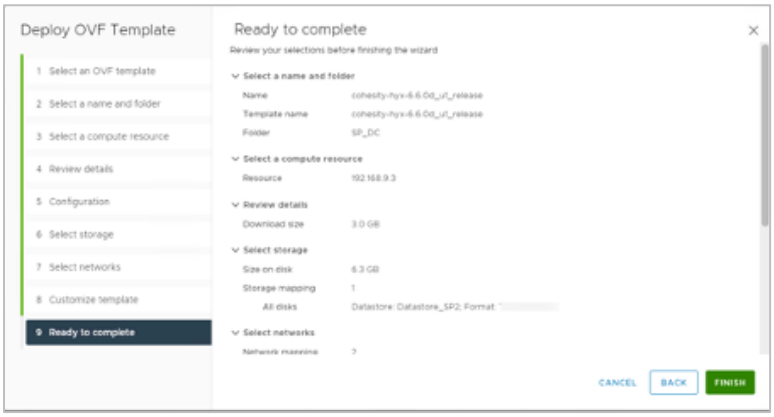

16. Select the Network for DataNetwork and SecondaryNetwork and IP Allocation settings. Click **NEXT**.
    a. **Static**: You have to manually provide the IP address details and update the DNS information after the deployment in /etc/resolv.conf.
    b. **DHCP**: It will automatically take the IP address detail and fetch the DNS details.



17. In the Customize template window, leave it blank if DHCP IP Allocation is selected in the previous step or provide the IP address details if Static IP allocation is selected.



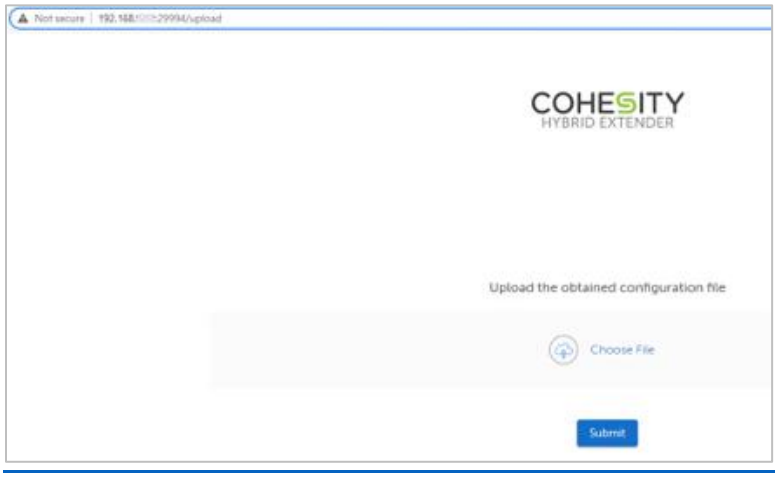

18. Review the information before the deployment and click **FINISH** to start the deployment.




19. Now that your hybrid extender VM is deployed, see the next step to register the hybrid extender.
20. Go back to the **Organization** page (Hybrid Extender) and under **STEP 2**, click **Download** to download the configuration file**.**

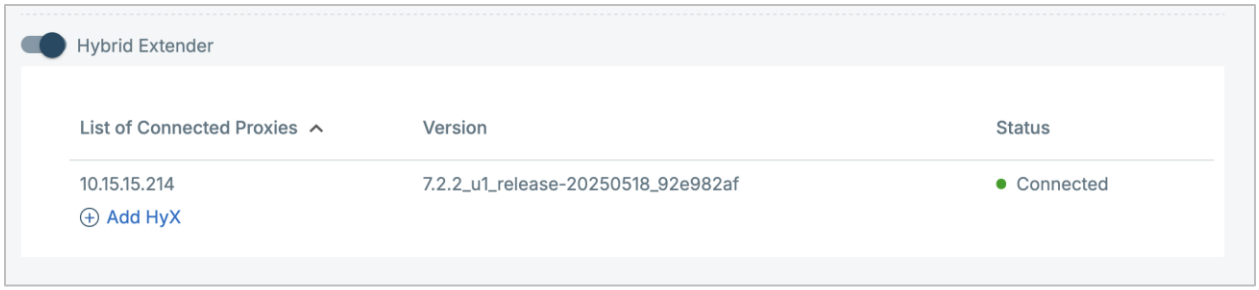
21. In the browser, enter the IP or FQDN with the hostname or IP address of the hybrid extender with port 29994. Click **Choose File**, upload the file and click **Submit**.

    URL: http://<IP_OR_FQDN>:29994/upload




> **NOTE**: The Hybrid Extender configuration file is editable. You can edit the file to include or exclude cluster VIPs, or replace the VIPs with the cluster hostname.

22. Now the Hybrid Extender status appears as Connected.



**NOTE**: If you have the reverse configuration or a different interface name, then the name of the interfaces can be accordingly specified in `customer_settings.json`. Once the VM is up, login into the HyX VM with the Credentials and create a `customer_settings.json` file in the `/home/cohesity/data/bifrost` directory.

1. Login in the HyX VM and navigate to the location.

   ```
   cd /home/cohesity/data/bifrost
   ```

2. Create a file `customer_settings.json` and enter the following information.

   ```
   vi customer_settings.json
   {
   "tenant_source_side_interface_name": "ens160",
   "cohesity_side_interface_name": "ens192"
   }
   ```

**IMPORTANT**: To achieve high availability, load balancing, good backup throughput, and a shorter backup window, you can also deploy more than one Hybrid Extender for your tenant organization for the adapters that support multi-streaming. The configuration file you upload on each Hybrid Extender VM must be unique. You should avoid uploading the same configuration file on different Hybrid Extender VMs. As the configuration file is editable, verify the Cohesity VIPs that the HyX connects to are non-overlapping across HyX when possible.

For example: If Tenant has 3 HyX, then three different jobs will use each HyX. Similarly, if one job is running, it will use one or more HyX depending on the adapter's compatibility with multistreaming. If the adapter supports multistreaming, then one job can use multiple HyX.

**NOTE**: See Appendix F to upgrade the Hybrid Extender from Version 1 to Version 2.



## Compare Service Provider and Tenant Administrator Privileges

For comparison, Table 9 below provides a summary of the privileges that are allocated to service provider administrators and tenant administrators.

Table 9: Service Provider vs Tenant Organization Administrator Privileges

| Resource | SP Administrator | | | | | Tenant Administrator | |
|---|---|---|---|---|---|---|---|
| | Create | Assign | Unassign | Delete | Can be shared across tenants? | Add/Create | Delete |
| **Storage Domain** | Yes | Yes | No | Yes | Yes | No | No |
| **View** | Yes | Yes | No | Yes[1] | No | Yes | Yes |
| **Full Source Tree** | Yes | Yes | No | No | No | Yes | Yes |
| **Partial Source Tree** | Yes | Yes | Yes | NA | Yes | No | No |
| **Protection Policy** | Yes | Yes | Yes | Yes | Yes | No | No |
| **Protection Group** | Yes | Yes | No | No | No | Yes | Yes |
| **VLAN** | Yes | Yes | Yes | Yes | No | No | No |
| **User/Group Management** | Yes | Yes | Yes | Yes | No[2] | Yes | Yes |

**NOTES**:

[1] The service provider admin cannot delete a View that is assigned to an organization but *can* delete any unassigned Views on the cluster.

[2] Users cannot be shared across tenants. However, if you are using Single Sign-on (SSO) groups, they *can* be shared.

# Isolate Tenant Networks Using VLANS

In any multi-tenancy deployment, it is crucial to isolate networks for each tenant, to maintain security for all tenants. In our solution, you can use virtual local area networks (VLANs) to isolate network traffic for each tenant organizations, by creating and assigning each tenant their own unique VLAN.

To configure a VLAN for each tenant:

1. Follow the instructions in the online Help to add a VLAN.
2. Assign the VLAN to a tenant organization. See Assign A VLAN.
3. (*Optional*) Configure a static route for each VLAN to route the VLAN network traffic via a specific interface. This step is required only when the endpoint is not within the same subnet range as the VLAN but can be reached via a VLAN interface that is configured on the cluster. See Add a Static Route in the online Help.

> **NOTE**: Cohesity Platform has added support for many more VLANs on the same cluster. Versions 6.5 and 6.6 support a maximum of 4,096 VLANs.

Now let's look at various deployment scenarios for Cohesity's Backup as a Service and the corresponding use case each scenario addresses, and how we can use VLANs with Cohesity to isolate tenant network traffic:

1. **Hosted Backup**. There are two ways to use VLANs and Cohesity to achieve BaaS for IaaS (Infrastructure as a Service): with *shared* or *dedicated* hypervisors.
   a. **Shared Hypervisor**. In Figure 13 below, Tenant 1's infrastructure (in blue) is co-hosted with Tenant 2's infrastructure (in orange), and both are backed up to Cohesity.

Figure 13: Use VLANs to Isolate Tenant Networks with Shared Hypervisors

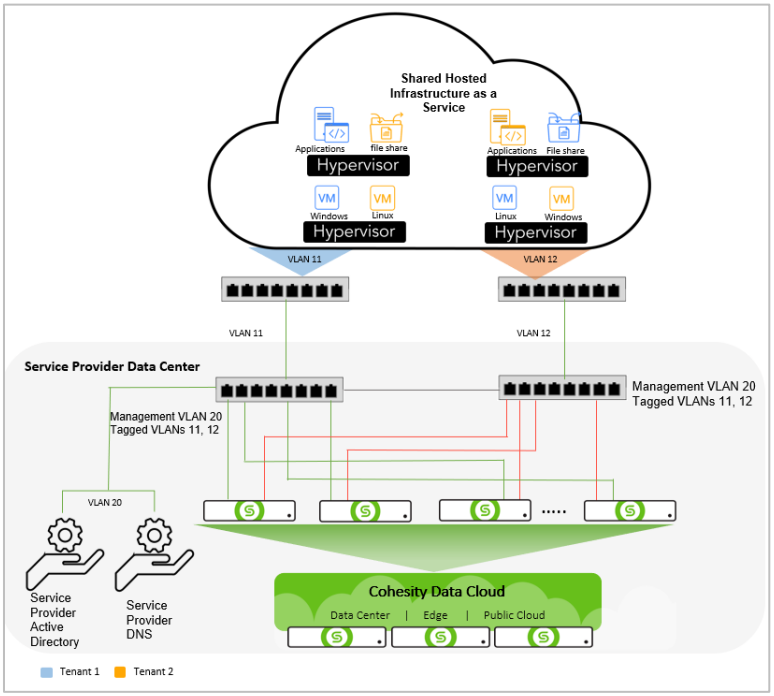


Table 10: Interface Group Configuration with VLAN Enabled

| Interface Group Name | Subnet | Gateway |
|---|---|---|
| intf_group1 | 10.0.20.0/24 | Node to Node, Cluster Create, NTP, DNS |
| intf_group1.11 | 10.0.11.0/24 | Tenant1 Backup |
| intf_group1.12 | 10.0.12.0/24 | Tenant 2 Backup |

b. **Dedicated Hypervisor**. In Figure 14 below, Tenant 1's infrastructure (in blue) is hosted on dedicated hypervisors and Tenant 2's infrastructure (in orange) is hosted on *other* dedicated hypervisors, and both are backed up to Cohesity.

Figure 14: Use VLANs to Isolate Tenant Networks with Dedicated Hypervisors

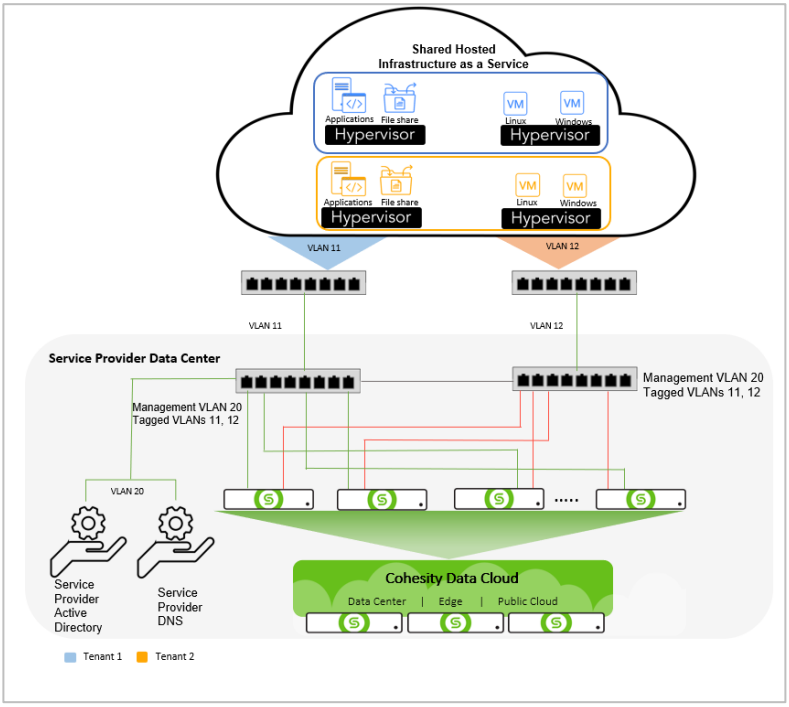



Table 11: Interface Group Configuration with VLAN Enabled

| Interface Group Name | Subnet | Gateway |
|---|---|---|
| intf_group1 | 10.0.20.0/24 | Node to Node, Cluster Create, NTP, DNS |
| intf_group1.11 | 10.0.11.0/24 | Tenant1 Backup |
| intf_group1.12 | 10.0.12.0/24 | Tenant 2 Backup |

2. **Local backup and Offsite Replication**. Figure 15 below illustrates how service providers can use VLANs and Cohesity to achieve managed BaaS and replication to the service provider.

Figure 15: Use VLANs to Deliver Managed BaaS and Replication

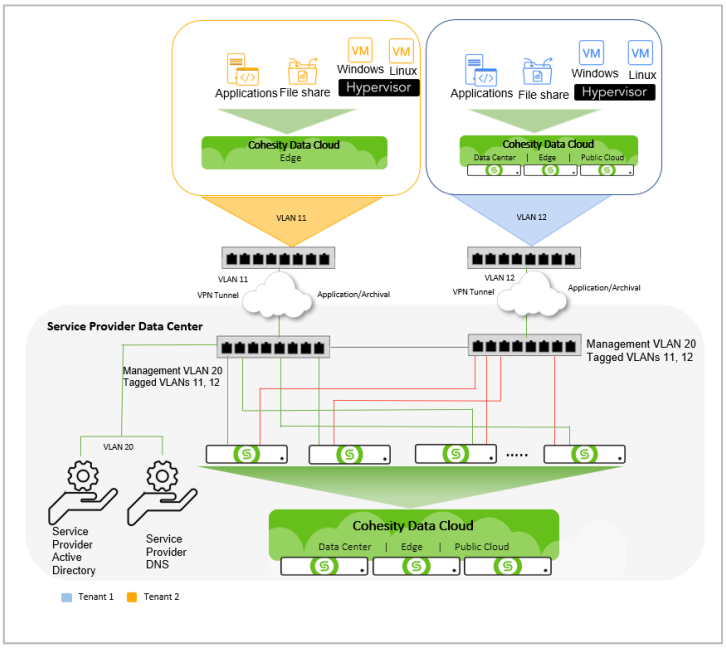



Table 12: Bond Configuration with VLAN Enabled

| Interface Group Name | Subnet | Gateway |
|---|---|---|
| intf_group1 | 10.0.20.0/24 | Node to Node, Cluster Create, NTP, DNS |
| intf_group1.101 | 10.0.11.0/24 | Replication |
| intf_group1.102 | 10.0.12.0/24 | Replication |

1. **Remote Backup**. Figure 16 below illustrates how service providers can use VLANs and Cohesity to achieve managed BaaS for the service provider.

Figure 16: Use VLANs to Deliver Managed BaaS

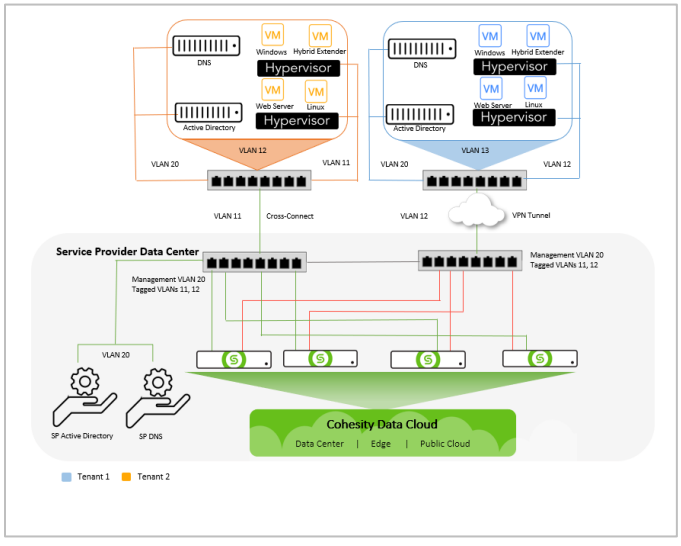


Table 13: Shows the bond configuration with VLAN enabled.

| Interface Group Name | Subnet | Gateway |
|---|---|---|
| intf_group1 | 10.0.20.0/24 | Node to Node, Cluster Create, NTP, DNS |
| intf_group1.11 | 10.0.11.0/24 | Tenant 2 Backup |
| intf_group1.12 | 10.0.12.0/24 | Tenant 1 Backup |

For more on adding and assigning VLANs per organization, see Enabling VLAN for Organizations.

For more on Cohesity Platform networking configurations, see Optimal Network Designs with Cohesity.



# Supported Multi-tenancy Workflows for Deployment Scenarios

Cohesity's BaaS service supports a wide variety of workloads across the deployment scenarios. The workloads supported for multi-tenancy depend upon the deployment scenario and corresponding network topology.

Find the specific workflows, their associated requirements, and steps for initial setup, backup, and restore under each deployment model:

- Hosted Backup
  - VMware (VMware vCenter, vCD)
  - Physical Servers
  - SQL Server
  - Oracle
  - Hyper-V
  - Nutanix Acropolis (AHV)
  - HyperFlex
  - SAP HANA
  - SAP Sybase ASE
  - NAS Backup (Isilon, NetApp, Generic NAS)
  - Cohesity View
  - Remote Adapter
  - Microsoft Active Directory, Exchange OnPrem
  - Office 365 (Outlook, OneDrive, SharePoint)
  - AWS Cloud Workflows
- Local Backup
- Remote Backup
  - VMware ESXi/vCenter
  - Physical Servers

## Hosted Backup – Workload Workflows

As outlined in Hosted Backup Deployment above, hosted backup can have different network topologies. These topologies govern how the backup and restores happen for different workloads.

### VMware

Table 13 captures the supported workflows for VMware workloads. It elaborates on the steps for different backup and restore workflows and the corresponding requirements. For all the workflows, both tenant-reachable and tenant-isolated networks are supported, with the noted considerations below the table.



Table 14: Hosted Backup for VMware Workloads

| VMWARE | | | |
|---|---|---|---|
| **Workflows** | **Steps** | **Tenant-reachable Network** | **Tenant-isolated Network** |
| **Initial Config** | 1. Cohesity connects to the vCenter.<br>2. Cohesity discovers the VMs on the vCenter/vCD. | Supported | Supported |
| **VM Backup** | 1. Cohesity connects to the vCenter.<br>2. Cohesity creates VM snapshots and copies the data to Cohesity using VMware vSphere Storage APIs – Data Protection (fka VMware VADP). | Supported | Supported |
| **VM Restore** | 1. To restore a VM, Cohesity clones the backed up VM onto an internal Cohesity NFS View that is exposed to the shared VLAN.<br>2. Cohesity makes API calls to send the NFS View path to vCenter, and vCenter uses the path to mount the internal NFS View.<br>3. Once the NFS View is mounted, the cloned VM is vmotioned on to the datastore on the restore target. | Supported [1] | Supported [1] |
| **VM File-level Restore - Windows** | 1. To restore a file on Windows, Cohesity uses the winexesvc.exe service (if it is installed) to restore the files to the VM.<br>2. Cohesity performs the restore using VMware APIs. | Supported | Supported [2] |
| **VM File-level Restore - Linux** | 1. To restore files, Cohesity clones the backed up files onto an internal NFS View. The View is exposed to the tenant VLAN in question.<br>2. Cohesity contacts the VM and pushes the Cohesity Linux agent to the VM. Once done, Cohesity connects to the agent and mounts the NFS View to the VM.<br>3. Once the NFS View is mounted, the files are restored to the VM. | Supported [3] | Supported [4] |

| VMWARE | | | |
|---|---|---|---|
| **Instant Volume Mount** | This requires the internal NFS View to be mounted on the ESXi host. | Supported | Supported [4] |
| **Crash-Consistent Recover for apps** | Same As **VM Restore Workflow** | Supported [1] | Supported [1] |
| **Virtual Disk Recovery** | 1. A new physical instance (VMDK) is extracted from the snapshot and stored temporarily in the View(datastore) on the Cohesity cluster.<br>2. New VMDK migrated from the View to the specified datastore.<br>3. Temporary View(datastore) deleted automatically. | Supported [1] | Supported [1] |

**NOTES**:

1. Prerequisites for VM Restore:
   - **DNS configuration**. Create a DNS A-record on the tenant DNS for the Cohesity VIP for the tenant. For restores, the ESXi host needs to mount an internal View from Cohesity. ESXi hosts should be able to resolve the VIP name to the IP address.
   - **File-level restores for Linux**. For file-level restores to Linux VMs, the internal NFS View needs to be mounted on the VM, so the VMs must be able to resolve the VIP name and mount the NFS View.
   - **Vmware Tools**: Vmware Tools must be installed.
   - Open the following ports:

| Port | Source | Target | Direction | Protocol | Usage Notes | Type Of Traffic |
|---|---|---|---|---|---|---|
| 111,2049 | ESXi host | Cohesity | Bidirectional | TCP | VM restores<br>File restores | Recovery |

2. If there is an issue with the Windows VM file-level restore (FLR), check for:
   - Any endpoint-protection software running on the machine can interfere with this workflow. As a workaround, allowlist the winexecsvc.exe service in the software.
   - If the FLR process still fails, check whether User Account Control (UAC) is enabled. If it is, disable UAC.

3. Prior to v6.6.0d, prerequisites for Linux VM FLR:
   - **DNS configuration**. Create a DNS A-record on the tenant DNS for the Cohesity VIP for the tenant. For restores, the VM needs to mount an internal View from Cohesity. The VM should be able to resolve the VIP name to the IP address.
   - **File-level restores for Linux**. For file-level restores to Linux VMs, the internal NFS View needs to be mounted on the VM, so the VMs must be able to resolve the VIP name and mount the NFS View.
   - Open the following ports:

| Port | Source | Target | Direction | Protocol | Usage Notes | Type of Traffic |
|---|---|---|---|---|---|---|
| 111,2049 | ESXi host | Cohesity | Bidirectional | TCP | VM restores<br>File restores | Recovery |

4. There are two solutions:
   - Download the file from Cohesity and copy the file manually to the machine.
   - From version v6.5.0a, Linux FLR will occur exclusively via the VMware API, using VMware Tools.

   For the Service Provider's Side NAT:
   - Specify the FQDN for the "Shared VLAN." It's the VLAN for which you select **Enable For All Organization**.
   - You need the tenant DNS to route the FQDN to the Cohesity cluster's NATed IP address.

   For details, see Appendix C: Handling Service Provider NAT Gateway.

**NOTE:** Starting with Cohesity version 6.5, you can perform Linux file- and folder-level restores using VMware tools. In that case, you don't need connectivity to the VMs.

## Physical Servers

Table 14 captures the supported workflows for Physical Server workloads. It elaborates on the steps for different backup and restores workflows and the corresponding requirements. Both tenant-reachable and tenant-isolated networks are supported for all the workflows, with the noted considerations below the table.

Table 15: Hosted Backup for Physical Server Workloads

| Physical Server | | | |
|---|---|---|---|
| **Workflows** | **Steps** | **Tenant-reachable Network** | **Tenant-isolated Network** |
| **Initial Config** | 1. Install the Cohesity agent on the physical server before registering it to the Cohesity cluster<br>2. Once registered, Cohesity contacts the Cohesity agent to establish an RPC (remote procedure call) communication on port 50051. | Supported | Supported [1] |
| **Physical Windows: Backup** | When backup starts, Cohesity contacts the physical agent on the server and instructs it to back up the filesystem and send the data to Cohesity. | Supported | Supported [1] |
| **Physical Windows: File and Volume Restore** | 1. To restore files, Cohesity clones the backed up files onto an internal SMB View. The View is exposed to the tenant VLAN in question.<br>2. Once done, Cohesity connects to the agent and mounts the SMB View to the VM.<br>3. The files and folders are then restored to the server. | Supported | Supported [2] |
| **Physical Linux: Backup** | When backup starts, Cohesity contacts the physical agent on the server and instructs it to back up the filesystem and send the data to Cohesity cluster. | Supported | Supported [1] |
| **Physical Linux: File and Volume Restore** | 1. To restore files, Cohesity clones the backed-up files onto an internal NFS View. The view is exposed to the tenant VLAN in question.<br>2. Once done, Cohesity connects to the agent and mounts the NFS View to the server.<br>3. The files are then restored to the server. | Supported | Supported [3] |
| **Instant Volume Mount** | This requires that the internal NFS View be mounted on the target host. | Supported | Supported [3] |

**NOTES**:

1. Make sure the physical servers are reachable from the Cohesity cluster. You can do so using 1:1 NAT of the server's private IPs to the NAT public IPs that are reachable from the Cohesity cluster. When registering the physical server, be sure to register it using the NATed IP.
2. There are two solutions for Windows file and volume restore:
   - Browse the backup metadata and download the file to your local machine and manually copy it to the server.
   - As the physical server IP already has a NATed IP, the restore should succeed. Because Windows AD authentication is required for a machine that is joined to the domain, the AD IP should also be NATed and reachable from the Cohesity cluster.
3. There are two solutions for Linux file and volume restore:
   - Browse the backup metadata and download the file to your local machine, and manually copy it to the server.
   - As the physical server IP already has a NATed IP, the restore should succeed, as long as the prerequisites for Linux VM FLR are met:
     - **DNS configuration**. Create a DNS A-record on the tenant DNS for the Cohesity VIP for the tenant. For restores, the VM needs to mount an internal View in Cohesity. The VM should be able to resolve the VIP name to the IP address.
     - **File-level restores for Linux**. For file-level restores to Linux VMs, the internal NFS View needs to be mounted on the VM, so the VMs must be able to resolve the VIP name and mount the NFS View.
     - Open the following ports:

| Port | Source | Target | Direction | Protocol | Usage Notes | Type of Traffic |
|---|---|---|---|---|---|---|
| 111,2049 | ESXi host | Cohesity | Bidirectional | TCP | VM restores<br>File restores | Recovery |

For the service provider's side NAT:

- Specify the FQDN for the "Shared VLAN."
- You need the service provider DNS to route the FQDN to the Cohesity cluster's NATed IP address.

For details, see Appendix C: Handling Service Provider NAT Gateway.



## SQL Server

Table 16 captures the supported workflows for SQL Server workloads. It elaborates on the steps for different backup and restore workflows and the corresponding requirements. Both tenant-reachable and tenant-isolated networks are supported for all the workflows, with the noted considerations below the table.

Table 16: Hosted Backup for SQL Server Workloads

| SQL Server | | | |
|---|---|---|---|
| **Workflows** | **Steps** | **Tenant-Reachable Network** | **Tenant-Isolated Network** |
| **VM with SQL Server Backup** | Create 2 jobs: infrastructure & DB data. (Deduplication eliminates redundancy.)<br>1. Step 1. Back up the VM as a VM.<br>2. Step 2. Back up the SQL DBs.<br>a. Install the SQL agent manually.<br>b. Register it as a physical server.<br>c. Register the physical server as a SQL server.<br>d. Create a backup job: file-, volume-, or VDI-based. | Supported | Supported [1] |
| **Create SQL backup of type "Volume-based"** | Same as above — choose volume-based in Step 2d. | Supported | Supported [1] |
| **Create SQL backup of type "File-based."** | Same as above — choose file-based in Step 2d. | Supported | Supported [1] |
| **Create SQL backup of type "VDI-Based"** | Same as above — choose file-based in Step 2d. | Supported | Supported [1] |
| **VM Restore of a Full SQL Server** | 1. Step 1. Restore the VM.<br>2. Step 2. Restore the DB. (See the steps in the below rows based on type of backup.) | Supported | Supported [(2,3)] |
| **Restore from File-Based Backup** | 1. The Cohesity cluster contacts the agent on the SQL server and creates a secure channel.<br>2. Cohesity cluster pushes the restore files to the target SQL server using the agent. | Supported | Supported [2] |

| SQL Server | | | |
|---|---|---|---|
| **Restore from VDI-Based Backup** | 1. The Cohesity cluster contacts the agent on SQL server and creates a secure channel.<br>2. Cohesity cluster pushes the restore files to the target SQL server using the agent. | Supported | Supported [2] |
| **Restore from Volume-Based** | 1. Cohesity puts the restore data in an internal SMB View and contacts the physical agent.<br>2. The agent mounts the SMB View on the target server.<br>3. Files are copied from the View and restored. | Supported | Supported [3] |
| **Test/Dev Clone** | 1. Cohesity puts the restore data in an internal SMB View and contacts the physical agent.<br>2. The agent mounts the SMB View on the target server.<br>3. Files are copied from the View and restored. | Supported | Supported [3] |

**NOTES**:

1. There are two solutions for SQL backup:
   a) Set up 1:1 NAT mapping for the SQL server. For step 2b and 2c above, be sure to use the NATed IP of the SQL server so that it is reachable by the cluster.
   b) The dump and sweep approach (with Cohesity's Hybrid Extender). Ask your SQL DBAs to dump the database nightly to a local drive. Then:
      i. Deploy the Hybrid Extender.
      ii. Register this server as a physical server and be sure to use the NATed IP of the SQL Server.
      iii. Create a physical server backup job.
2. SQL restore for file-based or VDI based backup doesn't require active directory connectivity.

   **Solution:** Set up a 1:1 NAT mapping for the SQL server for the cohesity agent to connect to the Cohesity cluster.
3. There are two solutions for SQL restore for volume-based and clones:
   a) **Solution 1**:
      i. Set up 1:1 NAT mapping for the SQL server.
      ii. If Active Directory has a NATed IP (AD reachable by Cohesity), enable **whitelist-all IP addresses** to access the Cohesity restore Views.

iii. If Active Directory doesn't have a NATed IP (AD not reachable by Cohesity), use local users for the restore flow.

b) **Solution 2:** If backup was performed using a dump and sweep approach, restore the files using the file-level restore workflow for physical servers.

For the service provider's Side NAT:

- Specify the FQDN for the "Shared VLAN."
- You need the service provider DNS to route the FQDN to the Cohesity cluster's NATed IP address.

For details, see Appendix C: Handling Service Provider NAT Gateway.

## Oracle

Table 17: Hosted Backup for Oracle Server Workloads

| Oracle Server | | | |
|---|---|---|---|
| **Workflows** | **Steps** | **Tenant-Reachable Network** | **Tenant-Isolated Network** |
| **VM with Oracle Server Backup** | Create 2 jobs: infrastructure and DB data. (Deduplication eliminates redundancy.)<br>1. Step 1. Back up the VM as a VM.<br>2. Step 2. Back up the Oracle DBs.<br>a. Install the Oracle agent manually.<br>b. Register it as a physical server.<br>c. Register the physical server as an Oracle server.<br>d. Create a backup job selecting active/passive node, Channels, and delete Archive log option. | Supported [1] | Supported [1] |
| **VM Restore of a Full Oracle Server** | 1. Step 1. Restore the VM.<br>2. Step 2. Restore the DB. (See the steps in the below rows based on type of backup.) | Supported | Supported [2] |
| **Recover Oracle Database (CDB and PDB)** | 1. The Cohesity cluster contacts the agent on Oracle and creates a secure channel.<br>2. The Cohesity cluster pushes the restore files to the target Oracle server using the agent with Cohesity Views | Supported [1] | Supported [1] |

| Oracle Server | | | |
|---|---|---|---|
| **Workflows** | **Steps** | **Tenant-Reachable Network** | **Tenant-Isolated Network** |
| **RecoverOracle TDE (Transparent Data Encryption) Database** | Same as above - select the configuration mechanism that is supported by Oracle | Supported | Supported [1] |
| **Granular Recovery of Oracle** | 1. Performed by RMAN script managed by admin.<br>2. Cohesity puts the restored data in an internal View and contacts the physical agent.<br>3. The agent mounts the View on the target server. | Supported | Supported [1] |
| **Instant Recovery - CDB/Oracle Database** | 1. Cohesity puts the restored data in an internal View and contacts the physical agent.<br>2. The agent mounts the View on the target server.<br>3. Files are copied from the View and restored by selecting the Migration option. | Supported | Supported [3] |

**NOTES**:

1. There are two solutions for Oracle backup:
   a) Set up 1:1 NAT mapping for the oracle server. Be sure to use the NATed IP of the SQL server or FQDN so that it is reachable by the cluster.
   b) **Allowlist-all IP addresses** to access the Cohesity Views.

   Open the following ports:

| Port | Source | Target | Direction | Protocol | Usage Notes | Type of Traffic |
|---|---|---|---|---|---|---|
| 50051 | Oracle Host | Cohesity | Bidirectional | TCP | Use for agent and agentless data transfer | Backup and Recovery |
| 111 | Server/Cluster | Cohesity | Bidirectional | TCP | NFS restores | Backup and Recovery |
| 2049 | Server/ESXi host | VIPs VLAN IPs | Bidirectional | TCP | NFS restores | Backup and Recovery |
| 11113 | Server (Windows) | Cohesity | Bidirectional | TCP | Backup to cluster | Backup |

   **NOTE**: See Ports for Communication and for best practice.

2. There are two solutions for SQL restore for volume-based and clones, as well:

   **Solution 1**:

   a) Set up 1:1 NAT mapping for the Oracle server.
   b) If Active Directory has a NATed IP (AD reachable by Cohesity), enable **allowlist-all IP addresses** to access the Cohesity restore Views.
   c) If Active Directory doesn't have a NATed IP (AD not reachable by Cohesity), use local users for the restore flow.

For the service provider's Side NAT:

- Specify the FQDN for the "Shared VLAN."
- You need the service provider DNS to route the FQDN to the Cohesity cluster's NATed IP address.

For details, see Appendix C: Handling Service Provider NAT Gateway.

# Local Backup – Supported Workloads

All Cohesity backup adapters are supported on the source cluster. The supported workloads for local backup with offsite replication are available in Supported Software in the online Help.

However, on a DR (disaster recovery) cluster that is enabled for multi-tenancy, only the following adapters are qualified:

- ESXi, vCenter, and vCloud Director
- Hyper-V
- Nutanix Acropolis (AHV)
- HyperFlex
- Physical Servers
- SQL on Physical Server
- Cohesity View
- Remote Agents
- NAS Backup (Isilon, NetApp, Generic NAS)
- Oracle
- SAP HANA
- SAP Sybase ASE
- Microsoft Active Directory, Exchange OnPrem
- Office 365 (Outlook, OneDrive, SharePoint)
- AWS Cloud Workflows

# Remote Backup – Workload Workflows

Cohesity version 6.6, we have added the support of following workload with the remote backup deployment with Hybrid Extender.

The prerequisites for remote backup of VMware and physical servers are:

1. Deploy Cohesity's Hybrid Extender on the tenant's vCenter server.
2. Upload a configuration file on the Hybrid Extender **Upload** page.

For remote backup deployments, Cohesity currently supports:

- VMware ESXi/vCenter workloads.
- Physical Server workloads.
- MSSQL
- Oracle
- SAP HANA



- SAP Sybase ASE
- NAS (Generic NAS, Isilon)
- External Targets of AWS, GCP, Oracle, and Azure for Cloud Archive

**NOTE**: See Supported Multitenancy Workflows for Hybrid Extender for supported Workflow with HyX V2.

## VMware ESXi/vCenter

When using the Hybrid Extender to back up data from a tenant's VMware vCenter to Cohesity, it is important to understand the backup workflow and considerations at play.

Figure 17 showcases a multi-tenancy setup where you can back up Tenant A and Tenant B using a remote backup workflow for VMware.

Figure 17: Remote Backup for VMware ESXi/vCenter

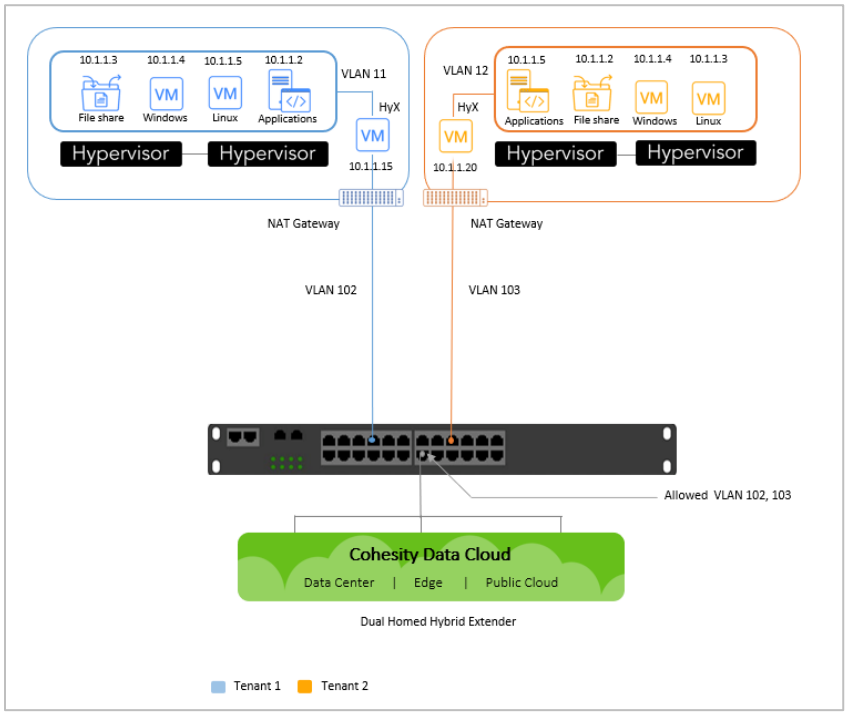



Table 17 captures the supported workflows for VMware workload for a remote backup deployment. It elaborates on the steps for the initial configuration and backup workflows. For all the workflows, both tenant-reachable and tenant-isolated networks are supported.

Table 18: Remote Backup for VMware Workloads

| VMWARE | |
|---|---|
| **Workflows** | **Steps** |
| **Initial Config** | 1. Cohesity connects to the vCenter.<br>2. Cohesity discovers the VMs on the vCenter/vCD. |
| **VM Backup** | 1. Cohesity connects to the vCenter.<br>2. Cohesity creates VM snapshots and copies the data to Cohesity using VMware vSphere Storage APIs — Data Protection (fka VMware VADP). |

## Physical Servers

Cohesity version 6.6 supports Physical server backup with HyX V2. You must install the physical agent on all the servers that you need to back up. The Hybrid Extender should be able to reach the Cohesity agent on the servers for backup workflow.

Figure 18 showcases a multi-tenancy setup where Tenant A and Tenant B can be backed up using the remote backup workflow for physical servers.

Figure 18: Remote Backup for Physical Servers

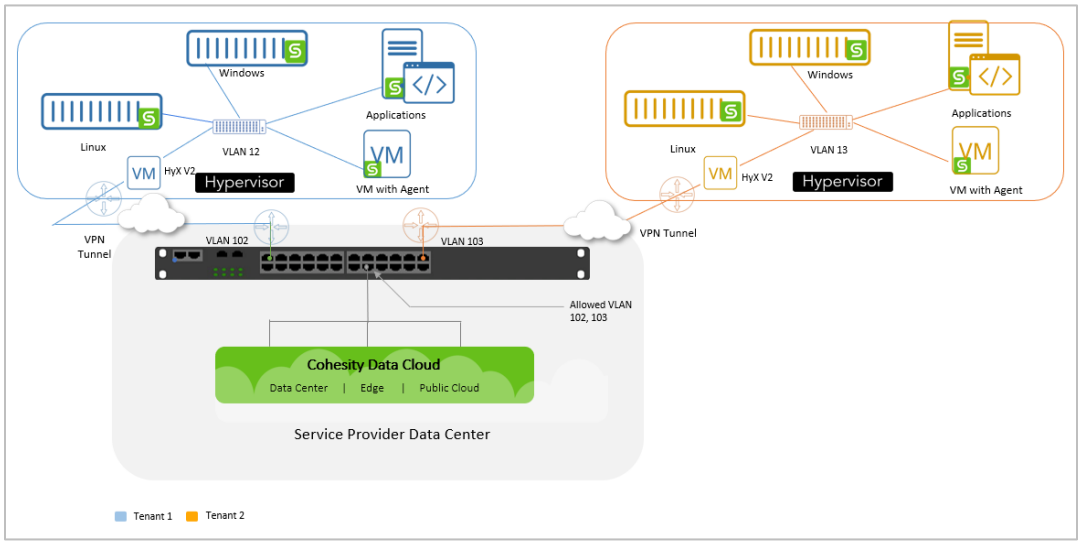



Table 18 captures the supported workflows for Physical Server workloads for a remote backup deployment. It elaborates on the steps for the initial configuration and backup workflows. For all the workflows, Cohesity supports both tenant-reachable and tenant-isolated networks.

Table 19: Remote Backup for Physical Servers

| PHYSICAL SERVER | |
|---|---|
| **Workflow** | **Steps** |
| **Initial Config** | 1. Install the Cohesity agent on the physical server before registering it to the Cohesity cluster.<br>2. Once registered, Cohesity contacts the Hybrid Extender, which contacts the Cohesity agent to establish an RPC (remote procedure call) communication on port 50051. |
| **Physical Windows: Backup** | When backup kicks in, the Hybrid Extender contacts the physical agent on the server and instructs it to back up the filesystem and send the data to it. The Hybrid Extender performs the source-side deduplication and sends the data to the Cohesity cluster. |

## SQL Server

Cohesity version 6.6 supports SQL database backup with HyX V2. We added support for backing up SQL database for volume-based, file-based, and VDI-based backups for remote backup deployment using Cohesity's Hybrid Extender. You must install the physical agent on all the servers you need to back up. The Hybrid Extender should be able to reach the Cohesity agent on the servers for backup workflow.

Figure 19 showcases a multi-tenancy setup where Tenant A and Tenant B can be backed up using the remote backup workflow for SQL servers

Figure 19: Remote Backup for SQL servers

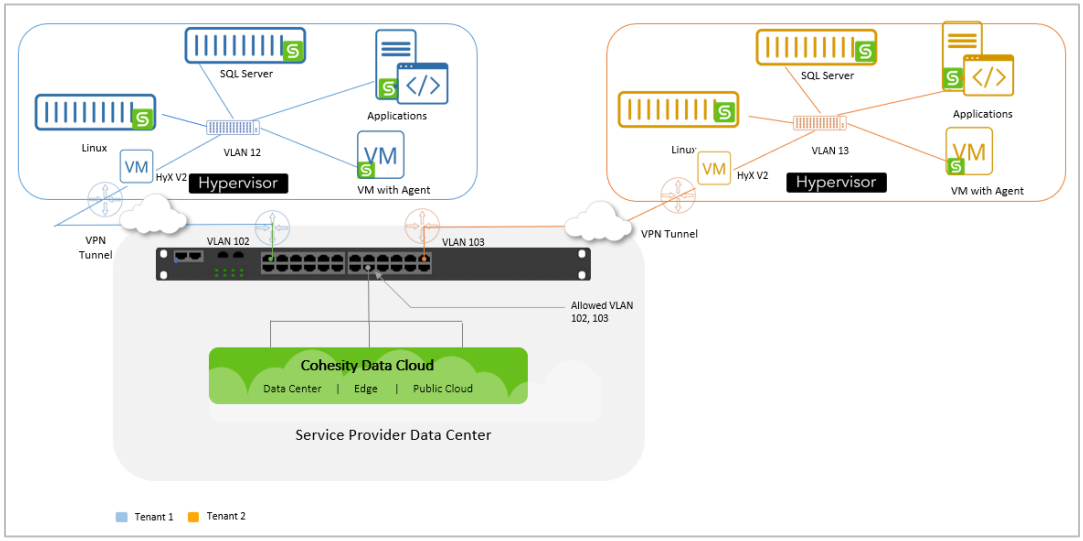


Table 20 captures the supported workflows for SQL Server workloads for a remote backup deployment. It elaborates on the steps for the initial configuration and backup workflows. For all the workflows, both tenant-reachable and tenant-isolated networks are supported.

Table 20: Remote Backup for SQL Servers

| SQL SERVER | |
|---|---|
| **Workflows** | **Steps** |
| **VM with SQL Server Backup** | Create two jobs: infrastructure and DB data. (Deduplication eliminates redundancy.)<br>Step 1. Back up the VM as a VM.<br>Step 2. Back up the SQL DBs.<br>a) Install the SQL agent manually.<br>b) Register it as a physical server.<br>c) Register the physical server as a SQL server.<br>d) Create a backup job: file-, volume-, or VDI-based. |
| **Create SQL backup of type "Volume-based"** | Same as above — choose volume-based in Step 2d. |
| **Create SQL backup of type "File-based"** | Same as above — choose file-based in Step 2d. |
| **Create SQL backup of type “VDI-Based”** | Same as above — choose file-based in Step 2d.<br>Allowlist the all the VIP in Global setting of Views. |
| **VM Restore of a Full SQL Server** | Step 1. Restore the VM.<br>Step 2. Restore the DB. (See the steps in the below rows based on type of backup.) |
| **Restore from File-Based Backup** | 1. The Cohesity cluster contacts the agent on SQL server and creates a secure channel.<br>2. Cohesity cluster pushes the restore files via HyX V2 to the target SQL server using the agent. |
| **Restore from VDI-Based Backup** | 1. The Cohesity cluster contacts the agent on SQL server and creates a secure channel.<br>2. Cohesity cluster pushes the restore files to the target SQL server via HyX V2 using the agent. |
| **Restore from Volume-Based** | 1. Cohesity puts the restored data in an internal SMB View and contacts the physical agent.<br>2. The agent mounts the SMB View on the target server via HyX V2.<br>3. Files are copied from the View and restored. |

| SQL SERVER | |
|---|---|
| **Test/Dev Clone** | 1. Cohesity puts the restore data in an internal SMB View and contacts the physical agent.<br>2. The agent mounts the SMB View on the target server Via HyX V2.<br>3. Files are copied from the View and restored. |

## Oracle Server

It elaborates on the steps for the initial configuration and backup workflows. For all the workflows, both tenant-reachable and tenant-isolated networks are supported with HyX V2.

Table 21: Remote Backup deployment for Oracle Server Workloads

| ORACLE SERVER | |
|---|---|
| **Workflows** | **Steps** |
| **VM with Oracle Server Backup** | Create 2 jobs: Infrastructure and DB data (Deduplication eliminates redundancy.)<br><br>Step 1. Back up the VM as a VM.<br>Step 2. Back up the Oracle DBs.<br>○ Install the Oracle agent manually.<br>○ Register it as a physical server.<br>○ Register the physical server as an Oracle server.<br>○ Create a backup job selecting active/passive node, Channels and delete Archive log option. |
| **VM Restore of a Full Oracle Server** | Step 1. Restore the VM.<br>Step 2. Restore the DB. (See the steps in the below rows based on type of backup.) |
| **Recover Oracle Database (CDB and PDB)** | 1. The Cohesity cluster contacts the agent on Oracle and creates a secure channel.<br>2. Cohesity cluster pushes the restore files to the target Oracle server using the agent with Cohesity Views. |
| **RecoverOracle TDE (Transparent Data Encryption) Database** | Same as above — select the configuration mechanism that is supported by Oracle. |
| **Granular Recovery of Oracle** | 1. Performed by RMAN script managed by admin.<br>2. Cohesity puts the restored data in an internal View and contacts the physical agent. |

| ORACLE SERVER | |
|---|---|
| | 3. The agent mounts the View on the target server. |
| **Instant Recovery -CDB/Oracle Database** | 1. Cohesity puts the restored data in an internal View and contacts the physical agent.<br>2. The agent mounts the View on the target server.<br>3. Files are copied from the View and restored by selecting the Migration option. |

# Generate Tenant Consumption Reports

Reporting is an essential part of Backup as a Service. It is how service providers can track, manage, and charge for their tenants' consumption of the service.

Different service providers charge on different metrics. For example:

- Per protected VM.
- Per front-end TB (such as logical data resident in the VM, or data transferred, and read).
- Per back-end TB (raw data or data after deduplication).

Cohesity provides many built-in reports that help you with planning, charge-back, compliance, and more. Some of the other benefits of Cohesity Reports include:

1. Schedule and receive reports through emails.
2. Filter reports based on type, operation, time frame, or tenant Organization.
3. Integrate with third-party business intelligence tools.

Cohesity provides required reports for Service Providers and Organizations:

1. Storage Consumed by Organizations
2. Storage Consumed by Storage Domains Report (Only for tenants)
3. Backup Summary
4. Clone and Recover VM Tasks Summary
5. Failed Objects
6. Protected Objects Heatmap (since 6.5.1 only)
7. Protection Runs Summary
8. Protection Summary by Object Type
9. Storage Consumed by Backups
10. Storage Consumed by Organizations
11. Unprotected/Protected VMs



Cohesity provides the ability to report on the storage metrics. Access to these reports is through multiple consumption points:

1. **Helios Reporting**. Available via Cohesity Helios and provides an aggregated view of all data under management across Cohesity clusters.

   > **NOTE**: Aggregated Reporting for Dark site customers is through our Helios Multi-Cluster Manager.

2. **Cohesity Platform Reporting**. Prebuild reports available via Cohesity Platform UI. The scope of these reports is at the cluster level.
3. **Custom Reporting**. Cohesity provides service providers a means to build their own Customized Reports. Customized reporting is possible via:
   - Helios Reporting APIs are available for customers to build their own reports. Additionally, we have published customizable sample scripts on Github.
   - Custom Reporting Database
   - Cohesity Platform APIs



# Built-in Reports for Service Providers

You can fetch or extract built-in reports that are particularly useful to BaaS service providers in one of the the following ways:

- Helios Reporting
- Cohesity User Interface (UI)

## Helios Reporting

Helios is Cohesity's SaaS-based management platform that provides a single dashboard and global management of all your Cohesity clusters. Helios provides multi-cluster management to actively manage all your clusters from a single dashboard, including multi-cluster monitoring, reporting, and orchestrated upgrades.

Helios has a growing number of built-in reports with data aggregation across various clusters, such as capacity usage across clusters. Currently, there are approximately 16 reports, and new reports are being added on a regular basis. Here are some examples:

- Storage Consumption by Organization: An aggregated summary of storage consumption per organization/tenant.
- Storage Consumption by Organization: An object-level storage consumption report to help the customer understand the consumption trend per object
- Storage consumption by Storage Domains: Reports on the consumption trend at a Storage Domain level.

Cohesity recommends using Helios Reports for your reporting needs. For more information, see Helios Reporting in the documentation.

## Cohesity User Interface (UI)

Cohesity (Single cluster) Built-in Reports are pre-built reports with filtering capabilities. You can generate reports on-demand and view them in different formats (HTML, CSV). You have the option to filter the report on date range and many other attributes (Protection Group name, VM name, status, etc.). You can also set up report schedules and event-triggered email messages.

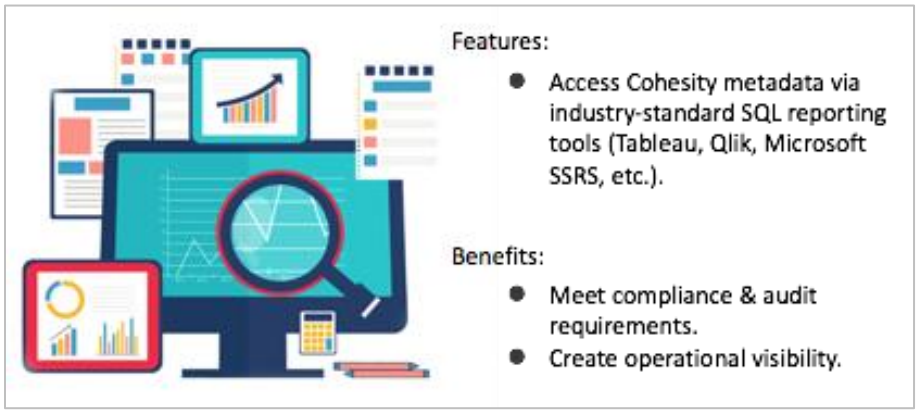
There are approximately two dozen built-in single cluster reports. The reports are grouped into five major groups:

- Capacity and Usage: Total capacity vs capacity in use.
- Design and Build: Backup sources, growth, duplicates, etc.
- Backup Operations: Protection Group reports.
- Backup Operations: Object (VMs backed up).
- Operational: Recovery, clone, and GDPR security operations.

# Custom Reports

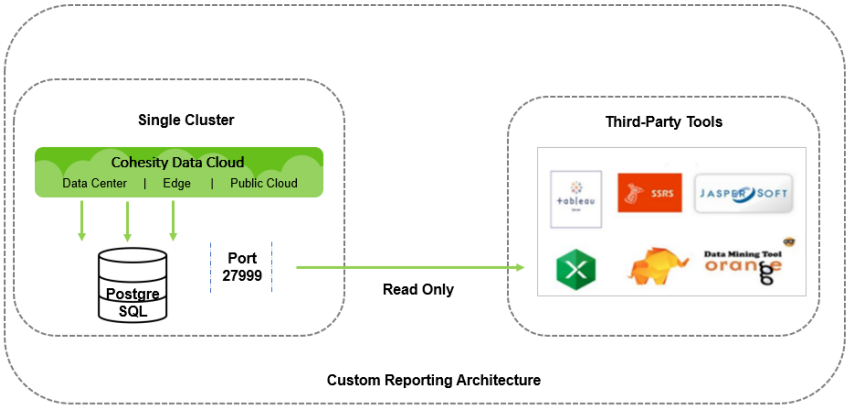
The Custom Reporting Database is a new feature built into the platform using a PostgreSQL database. An internal service called Groot collects statistics and metrics from various internal platform services and populates data into Postgres. To generate reports, service providers write SQL statements with the schema Cohesity has published. For more, see Custom Reporting in the online Help.

Figure 20: Use Cohesity's New Custom Reporting DB to Meet Every Reporting Need




The Service provides a vast array of new reports that a service provider can create as needed, using their internal business intelligence visualization tool with data from the PostgreSQL database, as illustrated in Figure 21.

Figure 21: Extract Custom Reporting Data for Third-party Visualization Tools



A Cohesity internal service performs ETL (Extract, Transform, Load) operations at a configurable frequency. During ETL operations, the service issues API calls to get statistics from other services, and stores the collated metadata in the custom database. The bootstrap run of the ETL process pulls the entire dataset to populate the custom database. In subsequent runs of the ETL process, the data refresh is incremental and only the delta is stored.

The types of data collected are:

- Details of objects and sources registered.
- Protection Groups configured.
- History of Protection Runs (archival, replication, backup, and restore).
- Performance metrics (IO, resources, and storage) of the cluster and the Protection Groups.
- Tenant and cluster (nodes and partitions) information.
- Backup schedule and Protection Policies.

See Cohesity Customer Reporting Solution Guide for more detailed information on the architecture and how to connect a business intelligence tool to the PostgreSQL database.

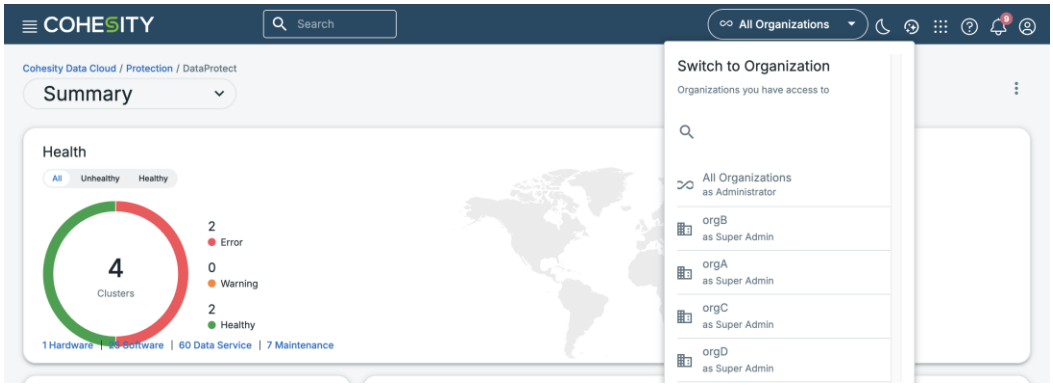


# Impersonate Tenants to Monitor, Diagnose, and Debug

Service Provider admins can “impersonate” organization administrators, and thereby preview and verify the tenant view of the org. The service provider administrator can enter impersonation mode and act as a tenant user to debug, diagnose, or assist with customer issues.

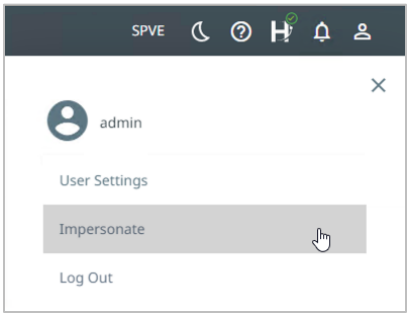
To impersonate a tenant login from **Cohesity Helios**:

12. Log in to **Cohesity Helios** as the Service Provider Admin user.
13. Click on the **All Organizations** drop down in the menu bar, and then click on the desired organization to impersonate.

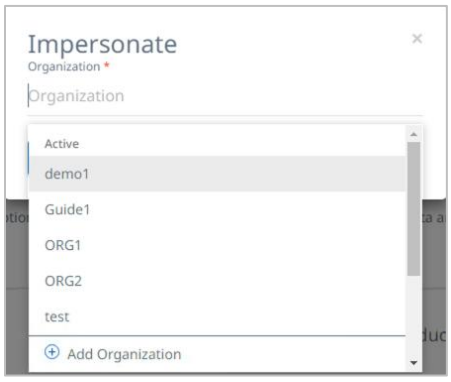



To impersonate a tenant login from **Cohesity Cluster**:

1. Log in to **Cohesity Cluster** as the service provider Admin user.
2. Click the profile icon in the top right, and then click **Impersonate** to see the tenant list.




3. Click the tenant organization name to log in.



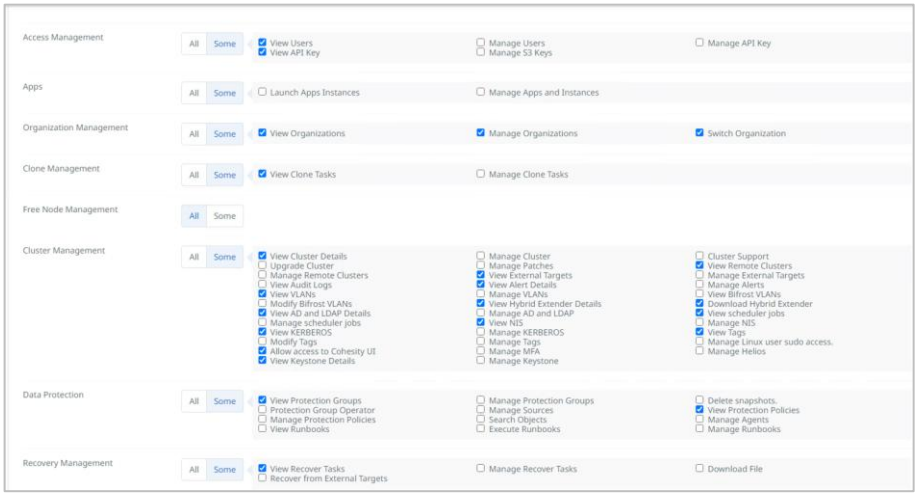
# User Role Privileges During Impersonation

Only users with “Organization Management > Switch Organization” privileges under their assigned role can impersonate tenants. The privileges available to service provider users remain the same at the organization level on impersonation. Only privileges available at tenant level are granted (see Example 2 below).

**Note:** For default roles, only a user with the Admin role at the cluster level can impersonate a tenant user. While a cluster admin is impersonating a tenant admin, the session has the same privileges as the tenant admin normally does.

**Example 1:** A service provider admin creates a custom role called “SP_test_role” and gives the user the following privileges:

- **Organization Management** > **Switch Organization**
- **Data Protection** > **View Protection Groups and View Protection Policies**




If a user with that “SP_test_role” role impersonates an organization user, for data protection, the user will only get the View Protection Groups and View Protection Policies privileges.

**Example 2:** A service provider admin user impersonates an organization user and the user gets tenant admin privileges. However, this user will not be able to create Protection Policies, as that are not included in the tenant admin’s privileges.

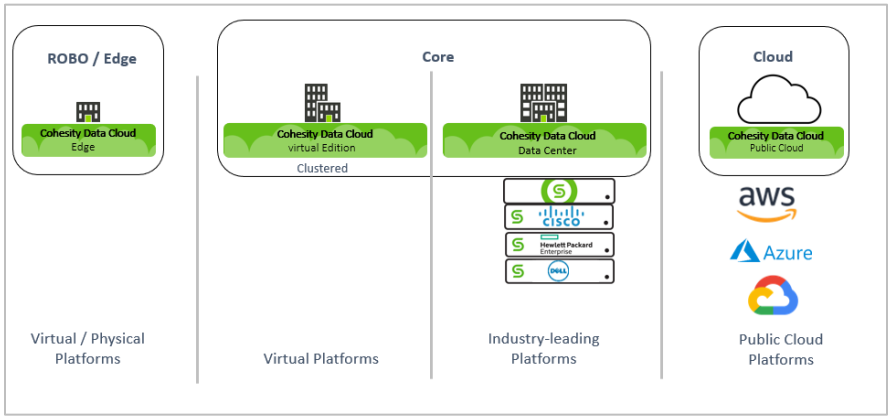
For more details on service provider and tenant administrator privileges see Compare Service Provider and Tenant Administrator Privileges.

# Supported Platforms

Cohesity is software-defined and is delivered as a software subscription priced on capacity utilization.

Cohesity can be provisioned on a choice of infrastructure platforms, from ROBO/Edge to core to the cloud, as shown in Figure 22 below. Core implementations are supported on both Cohesity Virtual Edition and industry-leading hardware, including the Cohesity C-Series, certified Cisco UCS, certified HPE Intel-based servers, and certified Dell servers. Cohesity also runs in the cloud, on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Starting from Cohesity version 7.2.2_u1, NGCE is supported for Organizations.

Figure 22: Supported Platforms for Cohesity



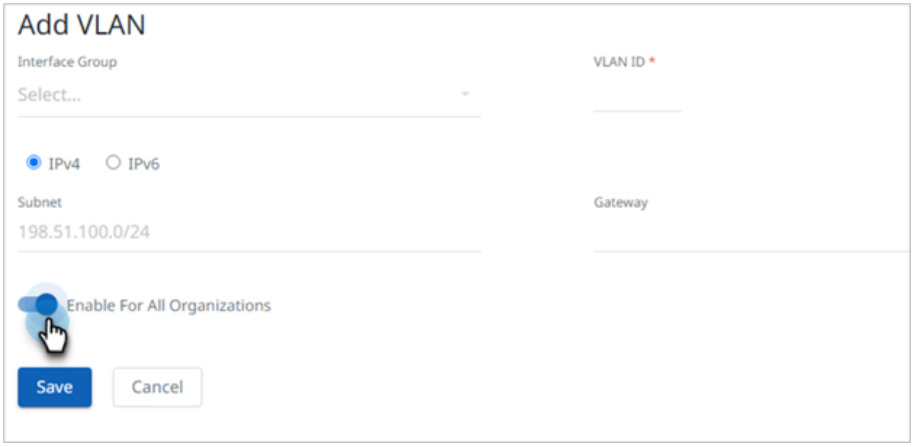

For an updated list of supported hardware platforms, see Initial Cluster Setup in the online Help.

For more on node compatibility for heterogeneous clusters with Cohesity version 6.6 and above, see Node Compatibility for Different Hardware Models in the online Help.

# Best Practice Considerations

Service providers who use Cohesity to deliver a BaaS solution should review the following recommendations:

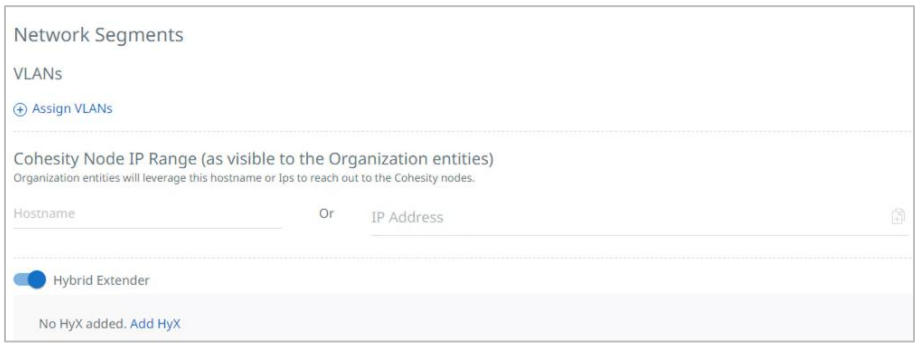
- To get better performance for VMware backups, use VMkernel ports (usually 10G) for backup instead of ESXi management (usually 1G) ports. To determine the port being used for backup and to make sure Cohesity uses the VMkernel Port for backup, see How to determine which vmkernel port is being used in a Cohesity VMware VM Backup in the Cohesity Knowledge Base.
- For a Hosted Backup solution with a shared hypervisor, service providers should make sure the VLAN carrying the backup traffic has the **Enable For All Organizations** option enabled. This ensures the same backup network can be used for backing up different tenants' data.




> **NOTE**:
> The "Enable for All Organization" option is not available for the cluster's default VLAN. Please create a new VLAN and share it across the organizations.

- Use VLANs to segregate traffic across different tenants. Each tenant can be assigned a VLAN.
- Use different VPN tunnels for different tenants if the tenants are remote and accessing the Cohesity cluster over the Internet. This is important for secure self-service restores.
- When replicating data between multitenant clusters, the same Organization ID and Storage Domain pairing must exist on both the transmitting and receiving clusters prior to running replication tasks.
- Follow the same practice when using CloudRetrieve; the same Organization ID and Storage Domains must exist on both clusters prior to running a CloudRetrieve download task.
- For service providers who are implementing a BaaS solution using Cohesity Data Cloud (Self-managed), Cohesity recommends that you segregate replication and backup traffic on the source cluster to avoid bandwidth issues. For more information, see Disaster Recovery as a Service (DRaaS) Solution Guide.
- Cohesity also recommends having a VPN connection between the source and DR clusters to set up replication across the clusters if the clusters are not using public IPs for replication communication.
- Alternatively, you can replicate over WAN without the need for a VPN connection.

- In Remote backup configuration, while downloading the HyX V2 configuration, make sure that there is no IP in Cohesity Node IP range in organization. Otherwise the HyX configuration file has only those VIP which are associated with the mentioned node IP.




- Create your naming convention of organizations to work with 9 characters.

  a) You cannot edit the Organization ID later. If the organization is deleted later, you cannot reuse the Organization ID.
  b) Use the same Organization ID across clusters.
  c) When replicating data between multi-tenant clusters, the same Organization ID and Storage Domain pairing must exist on both the transmitting and receiving clusters prior to running replication tasks.
  d) Follow the same practice when using CloudRetrieve; the same Organization ID and Storage Domains must exist on both clusters prior to running a CloudRetrieve download task.

- Enabling multi-tenancy for a cluster cannot be undone. You cannot revert the cluster to a single-tenancy state. Organizations can be deleted and deactivated.

  a) If CloudTier is on, the Cohesity cluster moves cold (rarely accessed) data to the designated External Target. Once CloudTier is on, it cannot be turned off.

# Appendix A: Data Isolation

To isolate data for each tenant, service providers can assign a dedicated Storage Domain to each tenant organization on the Cohesity cluster. With discreet Storage Domains for each tenant, service providers can also provide a separate encryption key for each assigned Storage Domain.

**NOTE**: Deduplication takes place at the Storage Domain level. If you use dedicated Storage Domains for each tenant, you will not be able to take advantage of global deduplication *across* tenants. Each tenant's data is still deduplicated against itself, but not against each other, which can decrease some space savings for service providers.



# Appendix B: Hybrid Extender Sizing

The Hybrid Extender is a pivotal part of the Backup as a Service solution. Because the Hybrid Extender handles the communication between the tenant environment and the Cohesity cluster sitting at the service provider data center, it is essential to size the Hybrid Extender VM.

The Hybrid Extender is delivered in the form of an OVA that can be deployed on a tenant's vCenter. The default configuration for the Hybrid Extender is:

Table 22: Hybrid Extender Sizing

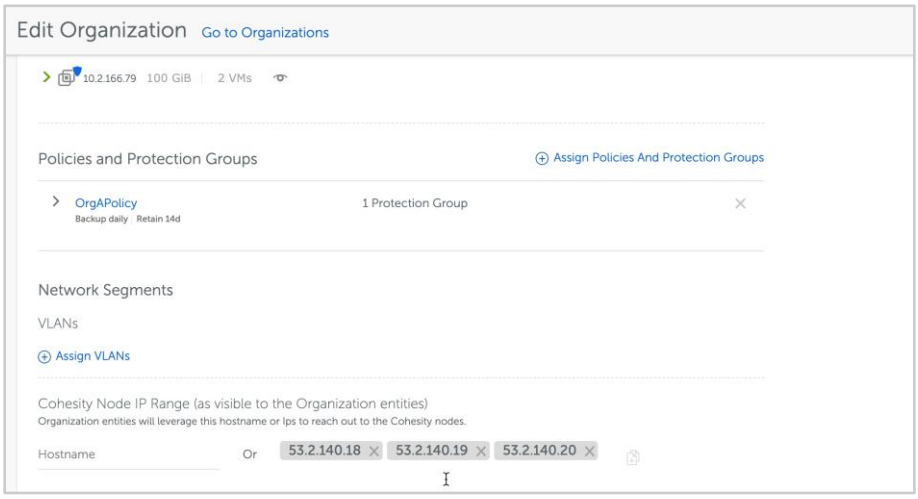
| Component | Configuration |
|---|---|
| CPU | 4 vCPUs |
| Memory | 4 GB |
| Hard Disk | 74 GB |

# Appendix C: Handling Service Provider NAT Gateway

Some service providers might have a NAT gateway in front of the Cohesity cluster, and the tenants will use the public IP address of the NAT to access Cohesity. On the NAT gateway, these public NAT IPs should be mapped to the Cohesity cluster's node VIPs.

During restore workflows, restore Views are exposed using the public IP address or the specified hostname so that tenants can reach the restore Views. Note that the Cohesity cluster's node IP range is visible to the Organization entities (tenants) on that cluster.

Figure 23: Edit Tenant Organization to Handle Service Provider NAT Gateway



# Appendix D: Single Sign-on with Multi-tenancy

On a Cohesity cluster that is enabled for multi-tenancy, you can configure Single Sign-on (SSO) at two different levels:

1. SSO for the service provider.
2. SSO for tenants.

## SSO for the Service Provider – Helios Workflow

You can now configure **Helios** to use an Identity Provider (IdP), such as Okta, for single sign-on (SSO) access. **Helios** must be added as an application to your IdP such as Okta. The SSO must then be configured along with the SSO URL and certificate file in **Helios**. After the integration, users can sign in to **Helios** using either the IdP sign in page or sign in with the SSO link in the **Helios** login page. For more information on configuring SSO for both Service Provider and Tenants, please refer Cohesity Helios **documentation**

## SSO for the Service Provider – Cluster Workflow

As a service provider, you can configure Single Sign-on at the cluster level. You can allow the administrator to use SSO to log in to Cohesity Platform. To configure SSO at the cluster level, see Manage Single Sign-On in the online Help.

> **NOTE**: A service provider can add SSO groups at the cluster level and assign them to one or more tenant organizations. This enables them to have a group of admins manage several organizations each.

## SSO for Tenant Organizations

A service provider or a tenant can configure Single Sign-on at the organization level. You can use different IdPs (Identity Providers) for service providers and for the organizations.

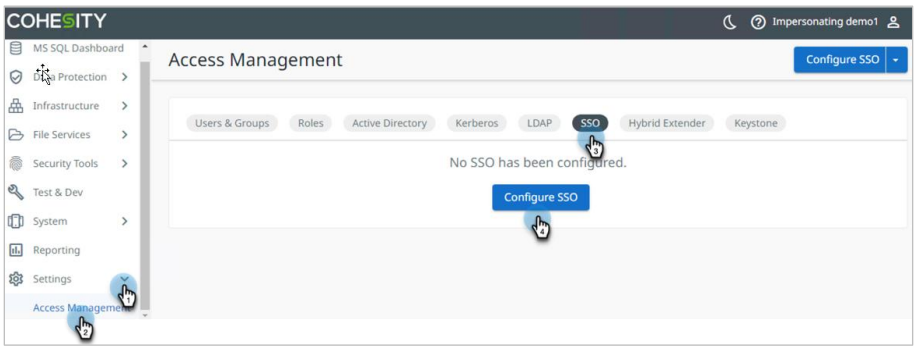
To configure SSO at the tenant level:

1. Configure the IdP (Identity Provider) to communicate with the **Cohesity cluster**. See Add an SSO Provider to Cohesity Cluster in the online Help.

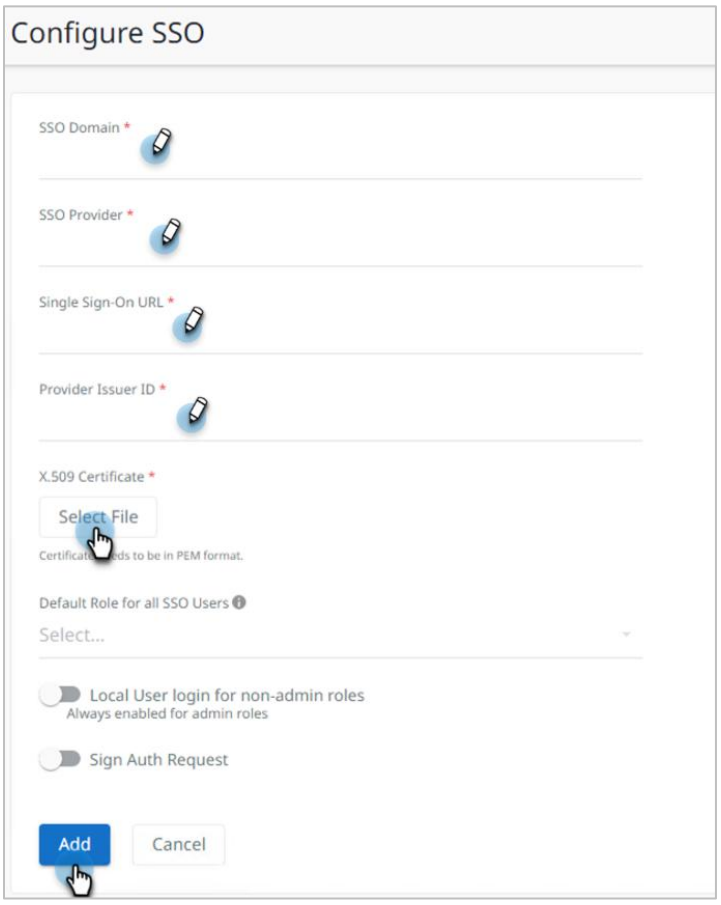
   > **NOTE**: Once configured, copy the **Logon URL**, **Provider Issuer ID**, and download the certificate in ".pem" format, then follow the steps below to configure the IdP at the Organization (tenant) level.

2. Log in to Cohesity as the tenant admin.

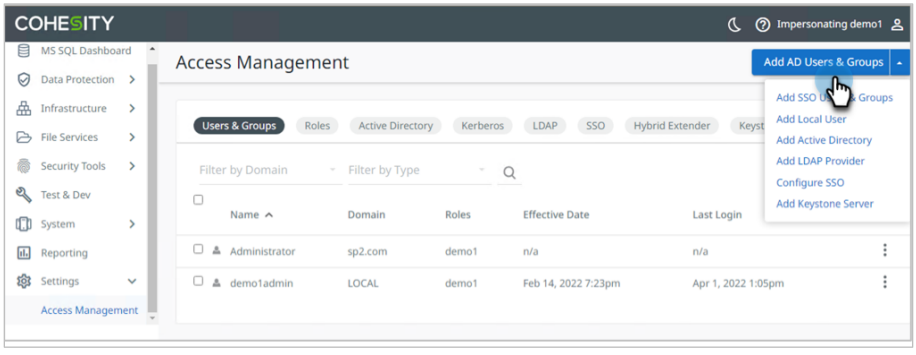
3. Navigate to, **Settings** > **Access Management** > **SSO** > **Configure SSO**.



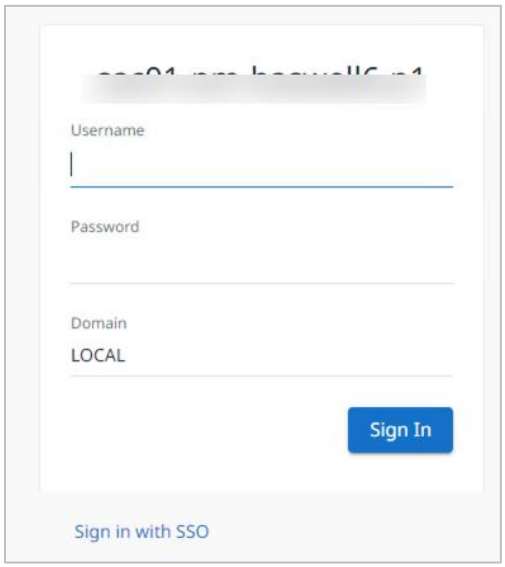

4. Enter the **SSO Domain**, **SSO Provider**, **Single Sign-On URL**, **Provider Issuer ID** and upload the .pem certificate file. Click **Add**.



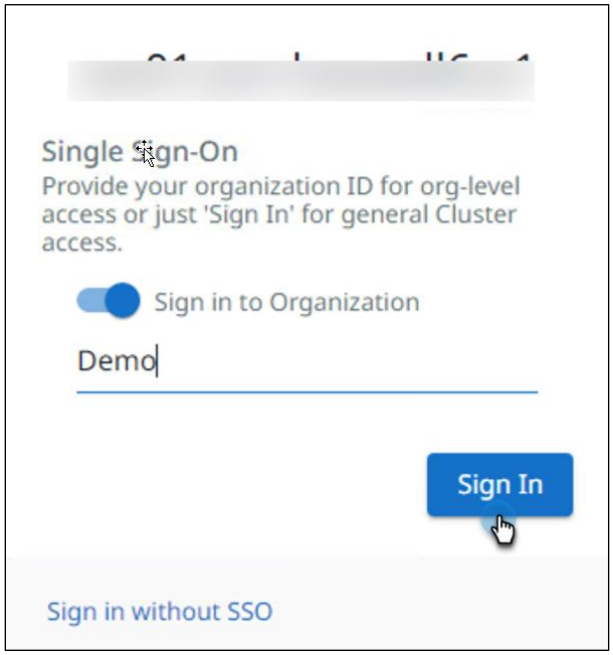

5. Once SSO is configured, click **Add Users & Groups** and assign them the appropriate roles.



6. To log in using Single Sign-on, click **Sign in with SSO**.




7. Enable **Sign in to Organization** to log in to a tenant organization using Organization-level SSO. Enter the Organization ID and click **Sign In**.



# Appendix E: Long-term Retention for Tenant Organizations

Long-term data retention is critical to organizations that seek to prevent data loss and meet security, legal, and compliance requirements. With CloudArchive and CloudRetrieve, customers can store data for long-term retention and disaster recovery. Cohesity enables customers to archive backup data to a designated External Target, such as cloud storage, NAS, or tape. For more, see About Cloud Archival in the online Help.

Cohesity provides a policy-based archival solution for backup data. In the Protection Policy, you can define the archival schedule, select the External Target, and specify the retention period for the data on the External Target.

Using the Cohesity, you can quickly archive data to multiple external targets such as:

- Public clouds
- Private clouds - S3-compatible device
- Any NAS-NFSv3 from storage vendors
- QStar managed tape libraries

As a service provider, you can register an external target and add the target to a policy that you can assign to an Organization for CloudArchive.

> **IMPORTANT**: Only service provider admins can create Protection Policies. Because archival configuration is part of a Protection Policy, this workflow doesn't exist for a tenant administrator.
>
> If you want your Organization Administrator to perform the Cloud Archive, you should create a protection policy with CloudArchive and assign the protection policy to the required Organization.

To make archival available to tenant organizations, the service provider administrator has to:

1. Add an External Target(s) to the Cohesity cluster. See Manage External Targets in the online Help.
2. Create Protection Policies and add an External Target to each of those Protection Policies.
3. Assign those Protection Policies to the respective organizations.

For more information, see About Policies and Protection Groups in the online Help.

## CloudArchive Workflows Supported for Multi-tenancy

The Cohesity CloudArchive features and workflows that are currently supported for multi-tenancy are listed in the Cohesity Product Documenation. Please refer the detailed documentation.



# Appendix F: Upgrading the Hybrid Extender

If you upgrade the Cohesity cluster from one maintenance release to another, you need not upgrade the Hybrid Extender. For example, if you upgrade the Cohesity cluster from 6.6.0c to 6.6.0d. However, Cohesity recommends that the version of the Cohesity cluster and the Hybrid Extender be the same.

## Considerations

- The hybrid extender and Cohesity cluster versions should be identical to best practices.
- If a tenant deploys multiple Hybrid Extender VMs, SMB, and NFS sessions do not failover to the next available Hybrid Extender VM. Cohesity Platform depends on the hypervisor hosting the Hybrid Extender VM to ensure high availability. If the hypervisor does not support high availability, I/O requests fail.
- Hybrid Extender does not support the following features:
  - S3
  - SMB Multichannel
  - Keystone
  - Kerberos client for NFS
  - SSO
  - NFS authentication
- Auto upgrade of Hybrid Extender is not supported.

## Prerequisite

Following are the pre-requisite to upgrade the Hybrid extender:

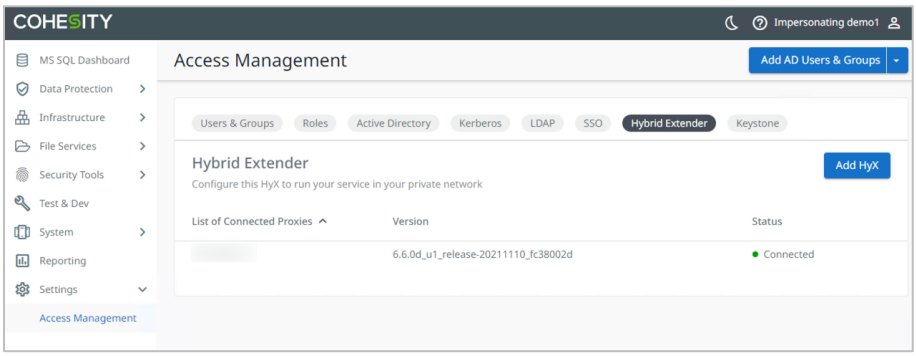
- Keep all the configuration backup of the Hybrid Extender before the upgrade.
- Ensure all the backup and replication jobs are stopped or in a pause state.
- Preserve all the network configurations which are edited manually on the Hybrid Extender.
- Keep note of the following:
  - Routing information
  - DNS entries (/etc/resolv.conf)
  - Hosts file (/etc/hosts)
  - /home/Cohesity/data/bifrost/customer_settings.json (applicable for version 6.6)
- Verify the port connectivity by using the Telnet command for all the required ports.



## Upgrade Hybrid Extender

To upgrade the hybrid, follow the steps below:

1. Take the snapshot backup of the Hybrid Extender.
2. Download and Deploy the Hybrid Extender.
3. Power off the running Hybrid Extender VM.
4. Power on the newly deployed hybrid extender.
5. Configure the Hybrid extender by uploading the configuration file.
6. You can preserve the old network setting of the hybrid extender and assign the same configuration.
7. Navigate back to **Settings > Access Management**. Click **Hybrid Extender** and verify the connectivity.




Hybrid Extender reflects its state as connected.

# Related Topics

See Cohesity Partner Portal for more recommended documentation in the *Service Provider* section:

- Service Provider Solutions
- Optimal Network Designs with Cohesity
- Cohesity Data Protection
- Cohesity Multi-Tenancy Guide
- Customer Reporting Deep Dive
- Custom Reporting Technical FAQ
- Cohesity Encryption Best Practices



# Your Feedback

Was this document helpful? Send us your feedback!

# About the Authors

**Punit Gupta** is a Senior Solutions Architect, STAT, and a part of Security COE at Cohesity. In his role, he focuses on Cohesity security products. His work includes POCs, testing, validation and providing solutions which meet customer requirements.

**Jedidiah Sonavane** is a Solutions Architect, STAT, and a part of Data Protect COE at Cohesity. He focuses on Service Providers/Organizations, Cloud Archive On-Prem, Gaia. His work proofs of concept, enterprise data protection, solution validation, solution design, testing, qualification, and ensuring software usability. He collaborates closely with teams to tailor solutions that meet customer needs while adhering to industry standards and best practices.

Other essential contributors included:

- Saurabh Singh, Staff Product Manager
- Yu-Shen Ng, Product Manager
- Palanivel Rajan, Product Manager
- Navaid Khan, Service Provider CTO
- Sourish Mazumdar, Senior Product Manager
- Mayank Narula, Engineering
- Piyush Sharma, Engineering

# Document Version History

| VERSION | DATE | DOCUMENT HISTORY |
|---|---|---|
| 3.3 | Nov 2025 | Content Updates |
| 3.2 | July 2024 | Republishing |
| 3.1 | July 2023 | Rebranding update |
| 3.0 | Oct 2022 | Major update |
| 2.0 | June 2020 | Major update |
| 1.0 | Aug 2019 | First release |

# 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.