COHESITY

Version 1.1

September 2019

Protect vCloud Director Environments with Cohesity DataPlatform

Bringing Simplicity to Multi-Tenant Data Protection

ABSTRACT

More organizations are using VMware vCloud Director to provide virtualized infrastructure as a service for multiple tenants seamlessly. To extend the infrastructure experience for tenants and service providers, Cohesity DataPlatform solves data protection challenges for vCloud Director, going beyond surface-level protection. Designed to integrate with VMware vCloud Director directly, Cohesity DataPlatform recognizes its constructs and provides protection and recovery at the vCloud Director level, organization level, and even at the vApp level.

Table of Contents

Figures

Tables

1 Introduction

When organizations use virtual infrastructure to streamline services and support multiple tenants, ensuring resources for all those tenants and reducing management overhead is a balancing act.

Many leading service providers and multi-tenant organizations use VMware® vCloud Director to provide flexible infrastructure as a service (IaaS) for their tenants. While simplifying allocation management, the additional logical layers pose a data protection challenge. Protecting these many moving parts – vApps, their respective VMs and data, their internal and external networking configuration – is a significant roadblock.

Cohesity DataPlatform supports in-depth protection for vCloud Director, going beyond surface-level protection. Cohesity DataPlatform has been designed to integrate with VMware vCloud Director, recognizing its constructs and providing protection and recovery at the vCloud Director level, organization level, or even at the vApp level.

Combining DataPlatform with vCloud Director in your environment provides additional benefits, strengthening flexibility, security, and business agility objectives.

In partnership with VMware, Cohesity brings the power of self-service to vCloud Director (vCD) tenants for backup and recovery with secure, native integration into the HTML UI. Integrated backup and recovery services for VMware vCloud Director streamlines operations and provides a rich tenant experience that allows Cohesity and VMware Cloud Provider Program partners to offer differentiated services.

This paper outlines the benefits of using Cohesity DataPlatform with vCloud Director, and the steps to configure the integration. For additional download, installation, and configuration deployment information, see our vCloud Director extension page on GitHub.

1.1 Audience

This solution guide is written for IT and VMware administrators familiar with VMware vCloud Director and Cohesity DataPlatform.

This guide assumes moderate knowledge of the following:

- VMware vSphere
- VMware vCloud Director
- Backup and recovery technologies

This guide also assumes you have an operating vCloud Director setup running with tenants.

1.2 Cohesity DataPlatform Architecture

Cohesity DataPlatform™ consolidates secondary data and applications, including backups, files, objects, test/dev, and analytics, on a single, software-defined platform. Inspired by web-scale architecture, Cohesity DataPlatform is a scale-out solution based on a unique distributed file system, SpanFS™. Cohesity DataPlatform modernizes and simplifies secondary data and application management by providing one platform for multiple secondary workloads.

Although most organizations begin their journeys to overcoming mass data fragmentation by simplifying data protection, Cohesity DataPlatform's flexible architecture allows easy expansion to additional use cases, further increasing operational simplicity and improved TCO (Total Cost of Ownership). Cohesity DataPlatform is a software-defined solution that works on-premises, on qualified Cisco, HPE, Dell or Cohesity C Series platforms, in the public cloud, as well as remote and branch offices on hypervisors of your choice, such as VMware and Hyper-V.

2 VMware vCloud Director

VMware vCloud Director (vCD) enables managed service providers to deploy, automate, and more effectively manage virtual infrastructure resources in a multi-tenant environment.

vCD acts as a management layer over server infrastructure, allowing cloud service providers and managed service providers to manage virtual data centers for multiple consumers of infrastructure resources.

2.1 Benefits of VMware vCloud Director

A prime benefit of vCloud Director is its capability to open up resources through a web portal, allowing for self-service management of resources. Policy controls supplement this self-service feature, providing the capability to set predetermined limits on resource consumption and access by users. The result is tenant self-sufficiency and fewer bottlenecks for both parties — the service provider and the consumer.

VMware vCloud Director supports overall business objectives by enabling:

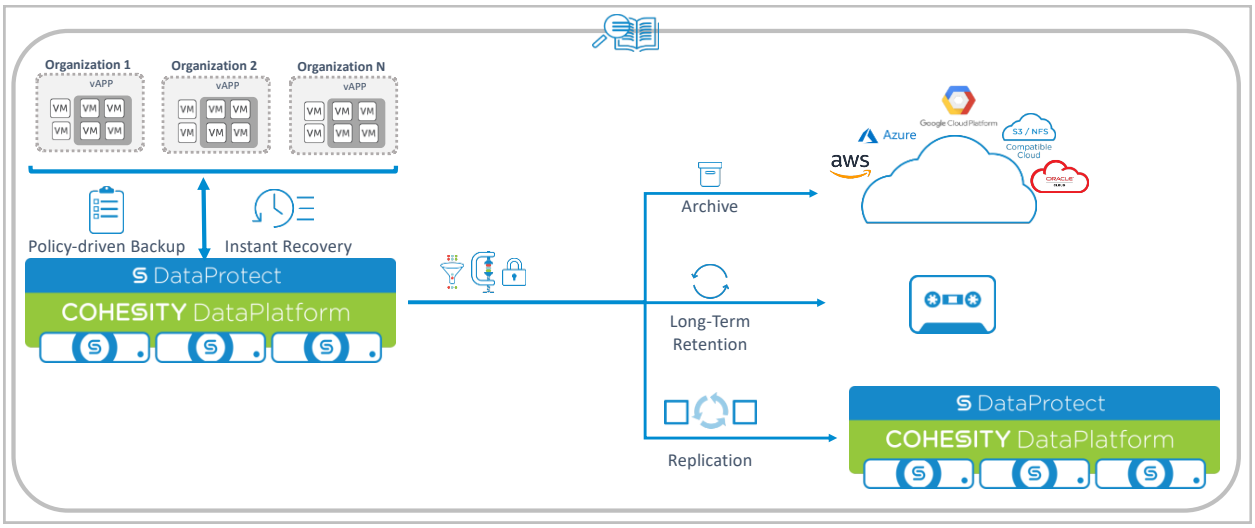
- Faster application provisioning — an organization administrator can provision resources, such as assign a network to VMs, without requiring service provider intervention.
- Internal resource conflict reduction — vCD converts physical resources into elastic, partitionable, virtual data centers, providing flexible control of resources by different teams.

3 Solution Overview: Integrated Data Protection

Leading service providers and multi-tenant organizations use vCloud Director to provide flexible IaaS (Infrastructure as a Service) environments for their tenants. VMware vCloud Director accomplishes this with a catalog-based self-service system along with policy controls. vCloud Director Administrators can establish organizations that allocate resources to their VMs, vApps, or groups of VMs, along with networking configuration. This enables granular and flexible resource control.

Cohesity DataPlatform has been designed to integrate with VMware vCloud Director, recognizing its constructs and providing protection and recovery at the vCloud Director level, Organization (vOrg) level, virtual data center (vDC) level, standalone VMs, or even at the vApp level, including protection for vApps and comprising VMs.

Figure 1: VMware vCloud Director with Cohesity DataPlatform Solution



3.1 Solution Benefits

By delivering granular and flexible end-to-end data protection for vCloud Director, Cohesity DataPlatform solves the data protection challenge for multi-tenant, self-service environments.

Backup-as-a-Service (BaaS) and disaster-recovery-as-a-service are available to tenants without the need for backend orchestration. Cohesity DataPlatform reduces management time and cost for managed service providers as well as enterprise administrations providing resources to multiple tenants.

These multi-tenant features are supplemented with per-tenant security as well as data isolation between individual tenants.

Cohesity DataPlatform delivers the following benefits for multi-tenant environments:

Table 1: Benefits of Cohesity DataPlatform in multi-tenant environments

FEATURES	BENEFITS
Converged data protection for multiple tenants	End-to-end data protection for vCloud Director with rapid Recovery Point Objectives (RPOs) in minutes and near-instant Recovery Time Objectives (RTOs).
Automated backup	Automated protection of vDCs and vApps, according to tenant needs.
Granular recovery	Ability to recover a subset of VMs, individual files and folders, or an entire vApp.
Tenant self-service	Ability to provide self-service data protection services to all tenants, with automated, role-based access controls, for flexibility and efficiency.
Global deduplication	Flexibility to achieve storage efficiency and reduce TCO by 50% or more through global variable-block, workload-agnostic deduplication across tenants or segregate deduplication for enhanced security.
Flexible chargeback reporting	Ability to track usage and custom SLA metrics for each tenant.
Per-tenant security	Self-service capabilities such as tenant-specific encryption keys, supplementing security features such as namespace isolation and per-tenant encryption of data at-rest and in-flight.

This guide takes you through the following tasks, helping you understand and get started with Cohesity DataPlatform data protection for VMware vCloud Director:

1. Configure vCloud Director with Cohesity DataPlatform.
2. Create Protection Jobs and Policies for vCloud Director Objects.
3. Recover vCloud Director objects.
4. Clone objects for Test and Dev.
5. Use archival and replication for disaster recovery and business continuity.
6. Use CloudTier for long-term retention and reduced TCO.

3.2 The Cohesity Approach to Backups and its Benefits

Cohesity DataPlatform, which includes API-first architecture and optimized ingest, produces immediate benefits for vCloud Director administrators.

3.2.1 API-first Architecture

Cohesity integrates with the vSphere suite of products seamlessly. There are no agents required on VMware vCloud Director or hypervisors under management.

3.2.2 Distributed, Parallel, and Workload-optimized Ingest

Cohesity distributes backup data to all the nodes in the cluster, in a true distributed sense, ingesting data with a parallelized approach. If you have a four-node cluster, data will be distributed across 4 nodes, providing the performance benefits of a scale-out architecture. Mega file ingestion is supported for both full and incremental backup. Some of the benefits of this approach in data protection include:

- Faster backup times
- Reduces the probability of VM stunning due to shorter backup windows.

4 Configure vCloud Director with Cohesity DataPlatform

Cohesity DataPlatform brings simplicity to multi-tenant data protection. It is seamless to configure vCloud Director with Cohesity DataPlatform.

4.1 Configuration Requirements

Your environment needs to meet several technical requirements before you can proceed with many of the workflows described. See these requirements in Appendix A.

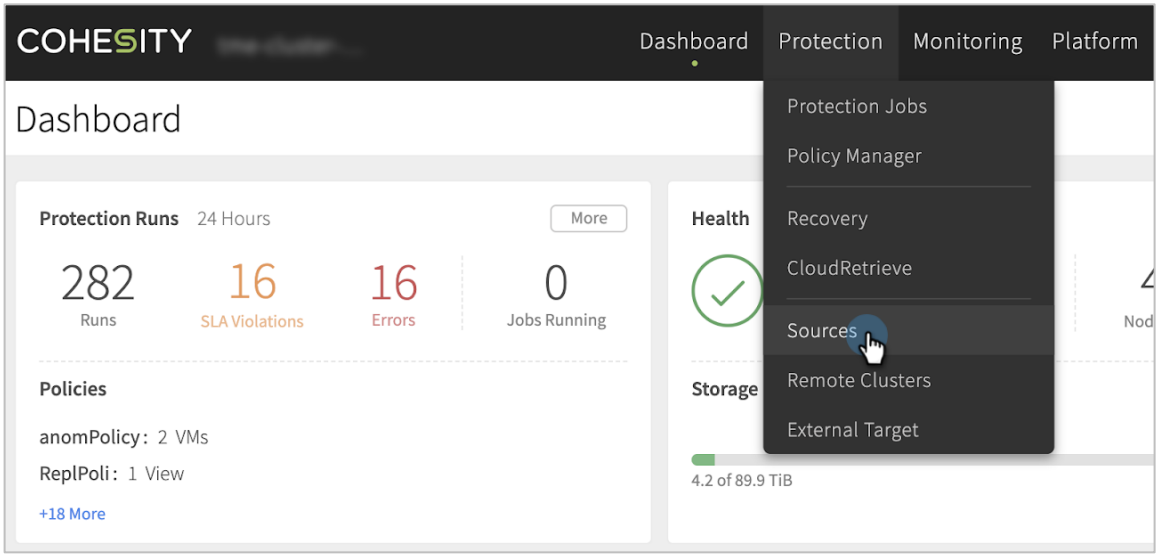
4.2 Register vCloud Director with Cohesity DataPlatform

Registering vCloud Director with Cohesity DataPlatform is simple — granular and SLA-based auto-protection is achieved by just entering the vCloud Director Hostname or IP address and the appropriate credentials.

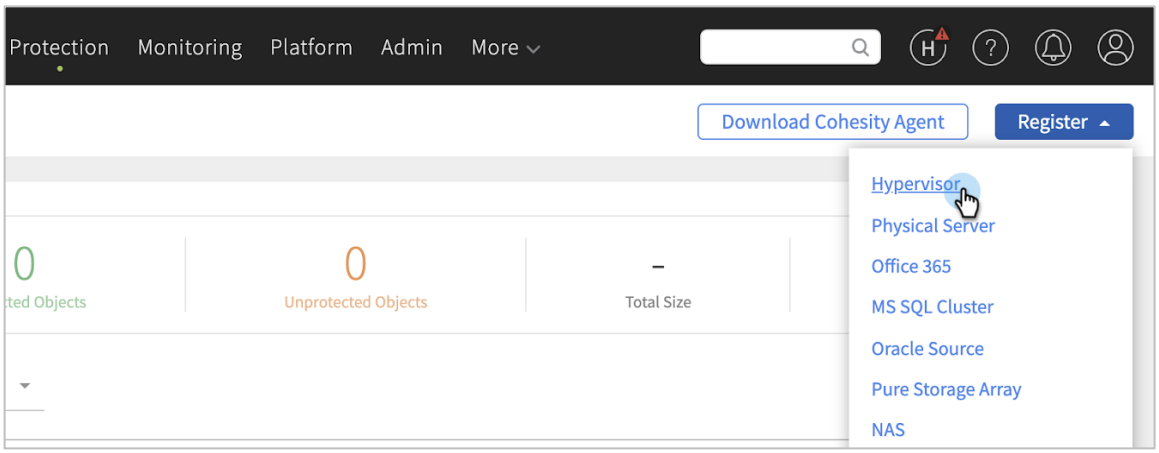
Registering a vCloud Director environment is as simple as connecting and authenticating individual vCenters under management.

To connect a vCloud Director environment:

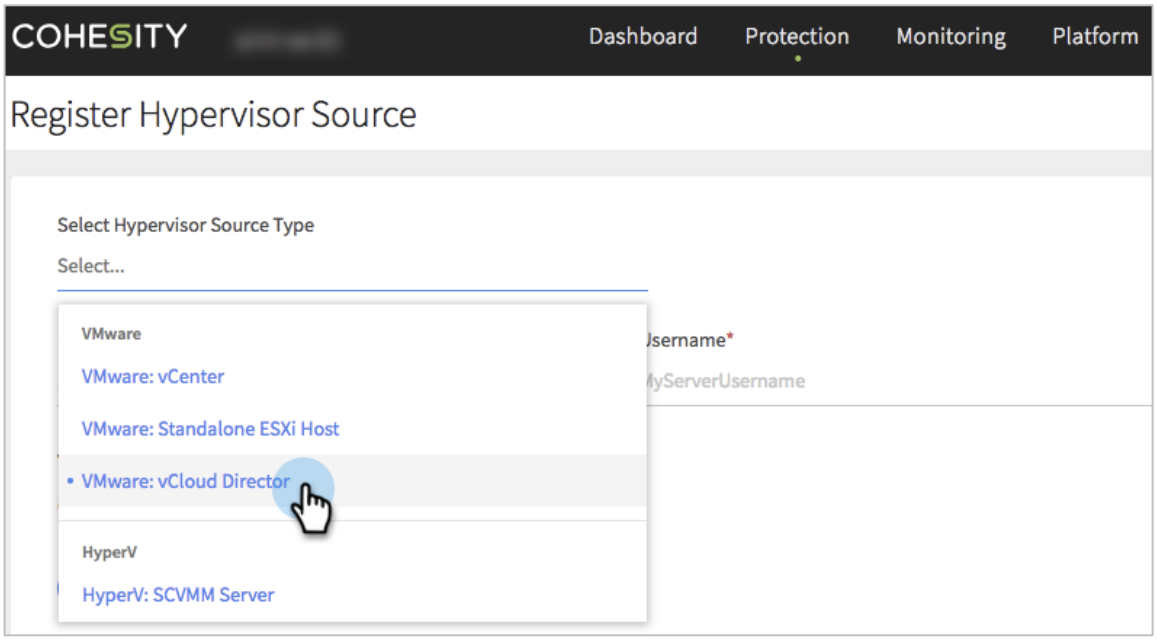
1. Log in to Cohesity DataPlatform.
2. Select **Protection** > **Sources**.



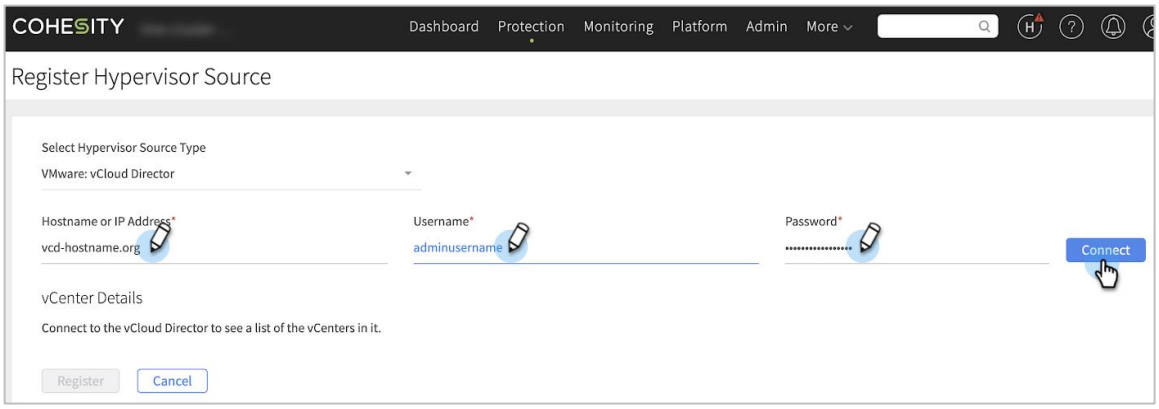
3. Select **Register** > **Hypervisor**.



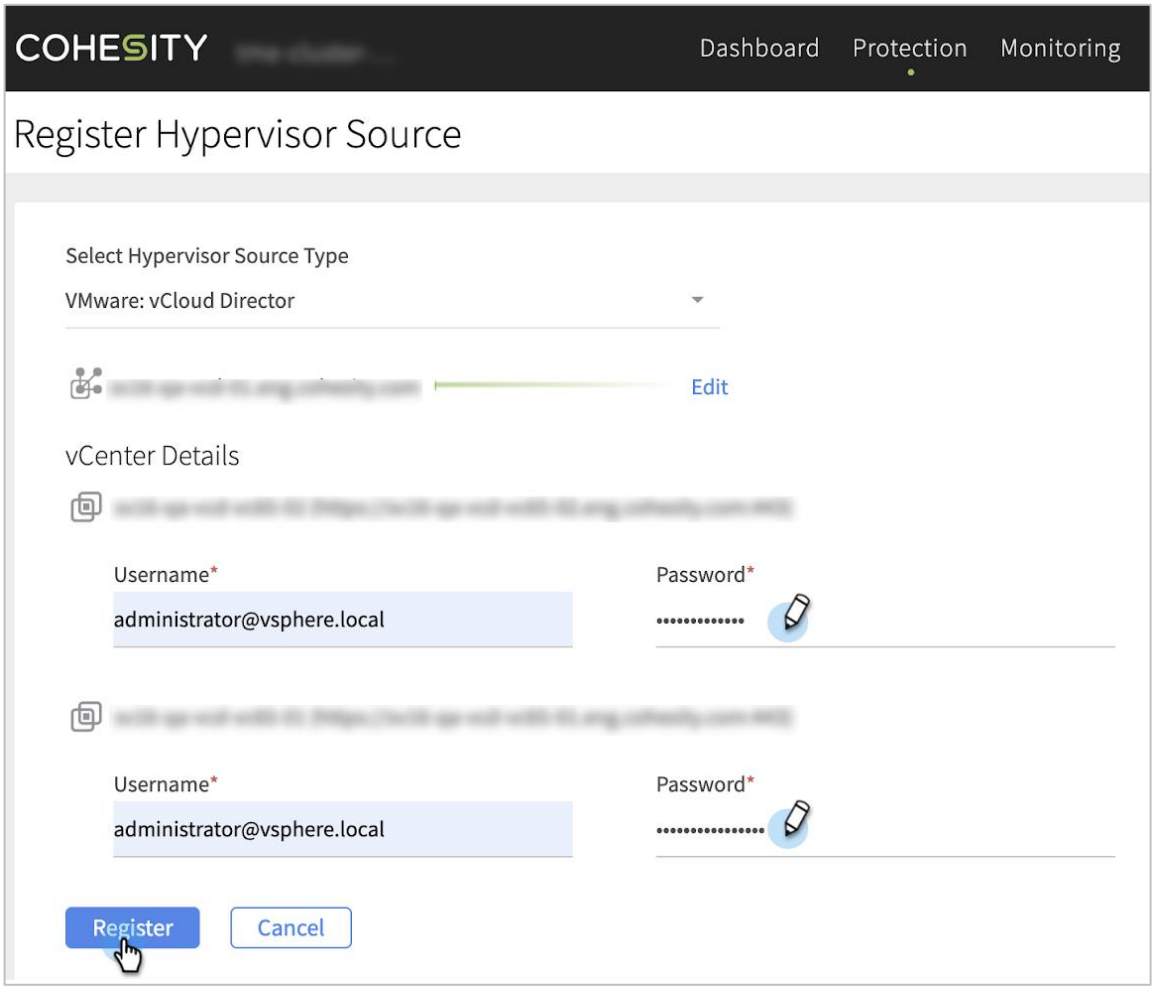
4. In the Register Hypervisor Source page, select **VMware: vCloud Director**.



5. Enter your vCloud Director Hostname or IP Address and credentials for registering the vCloud Director environment and click **Connect**.



6. Enter the credentials for vCenters under management and click **Register**.



5 Create Protection Jobs for vCloud Director Objects

Flexibility and agility are key paradigms for any organization, particularly with multi-tenant teams. Cohesity DataPlatform allows you to create Protection Jobs at any level of the vCloud Director environment.

5.1 Create a Protection Job: Protect Organizations, vApps, VMs, and More

Cohesity DataPlatform provides granular data protection at every level of vCloud Director:

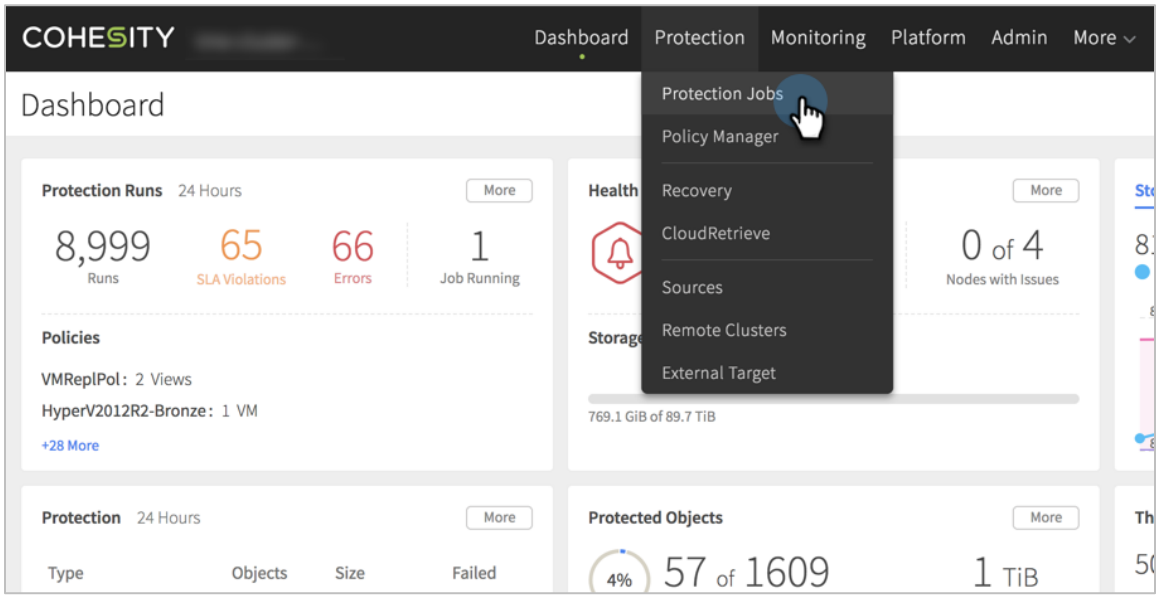
- Entire vCloud Director environments
- Individual virtual organizations
- Virtual data centers
- vApps
- Standalone virtual machines

By protecting vCD objects at different hierarchical levels, data protection complements multi-tenant objectives; a particular organization or virtual data center can be protected.

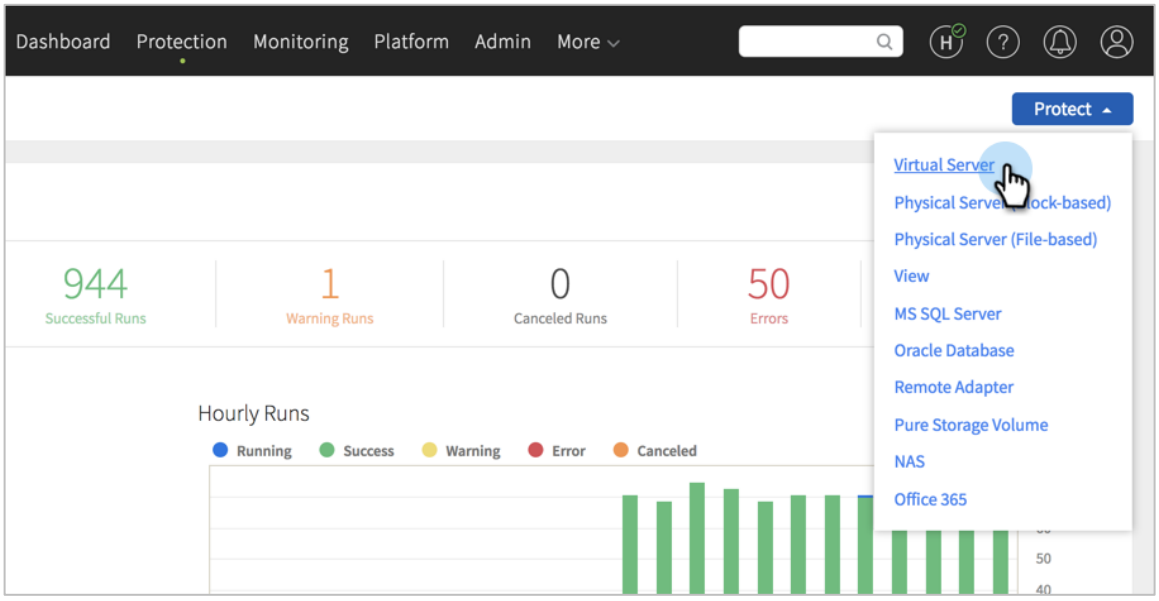
With Cohesity DataPlatform's additional multi-tenancy features, this granular level of data protection enables tenant self-service capabilities for data protection, lowering operation costs, and strengthening tenant efficacy.

To create a Protection Job:

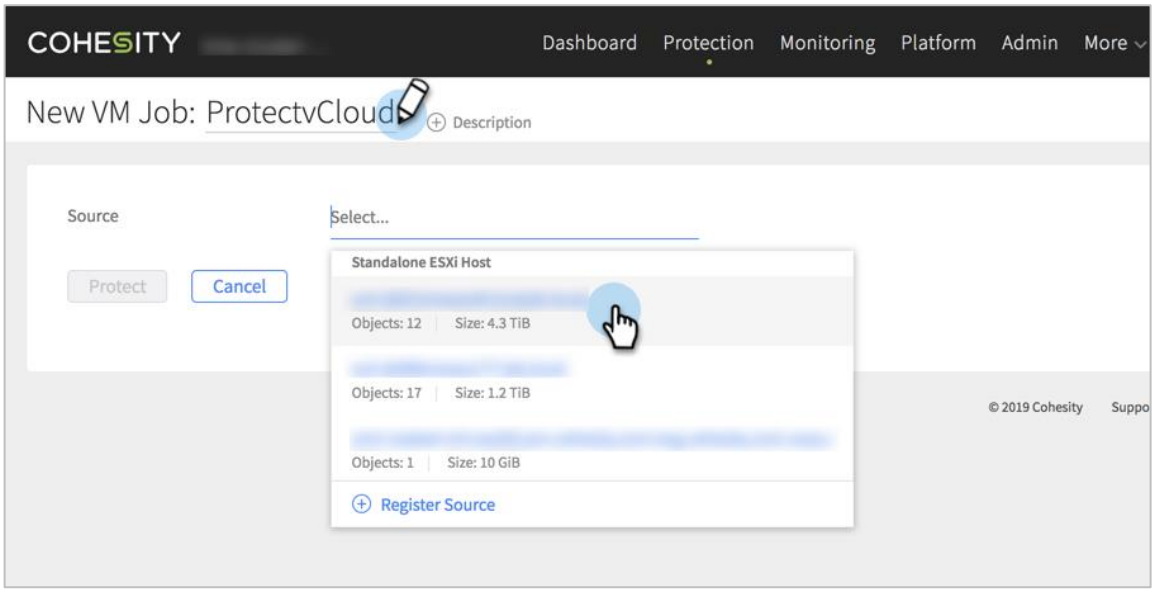
1. Log in to DataPlatform and select **Protection** > **Protection Jobs**.



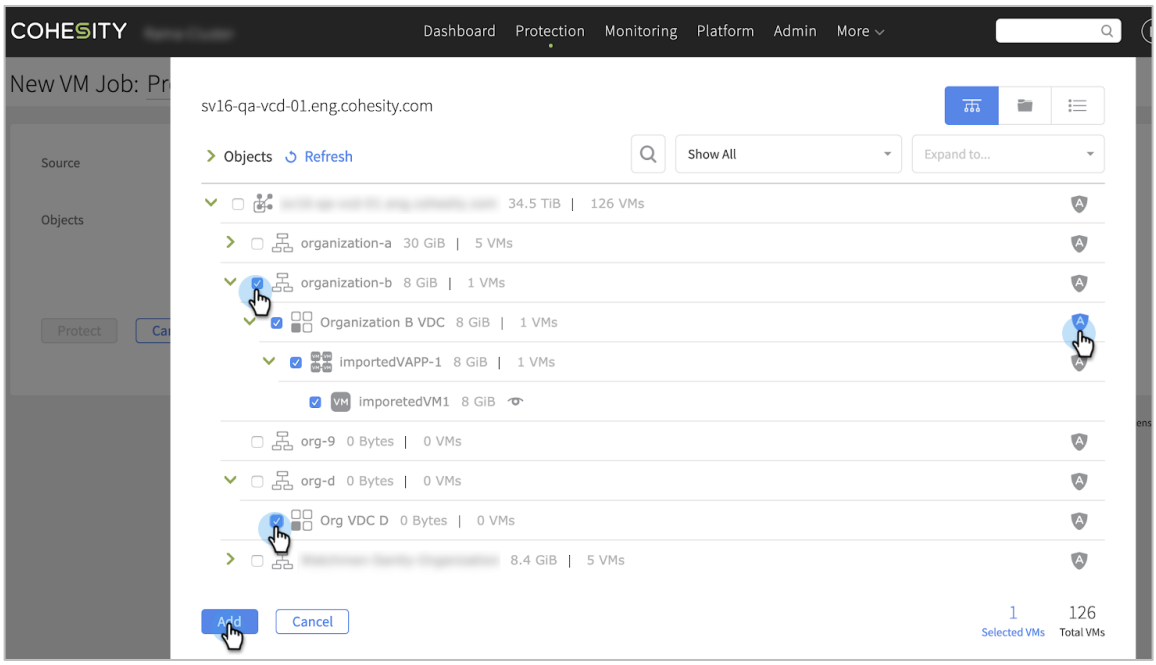
2. Select **Protect** > **Virtual Server**.



3. In the form, enter a **Name** for the New VM Job and select the **Source** that corresponds to your vCloud Director environment.



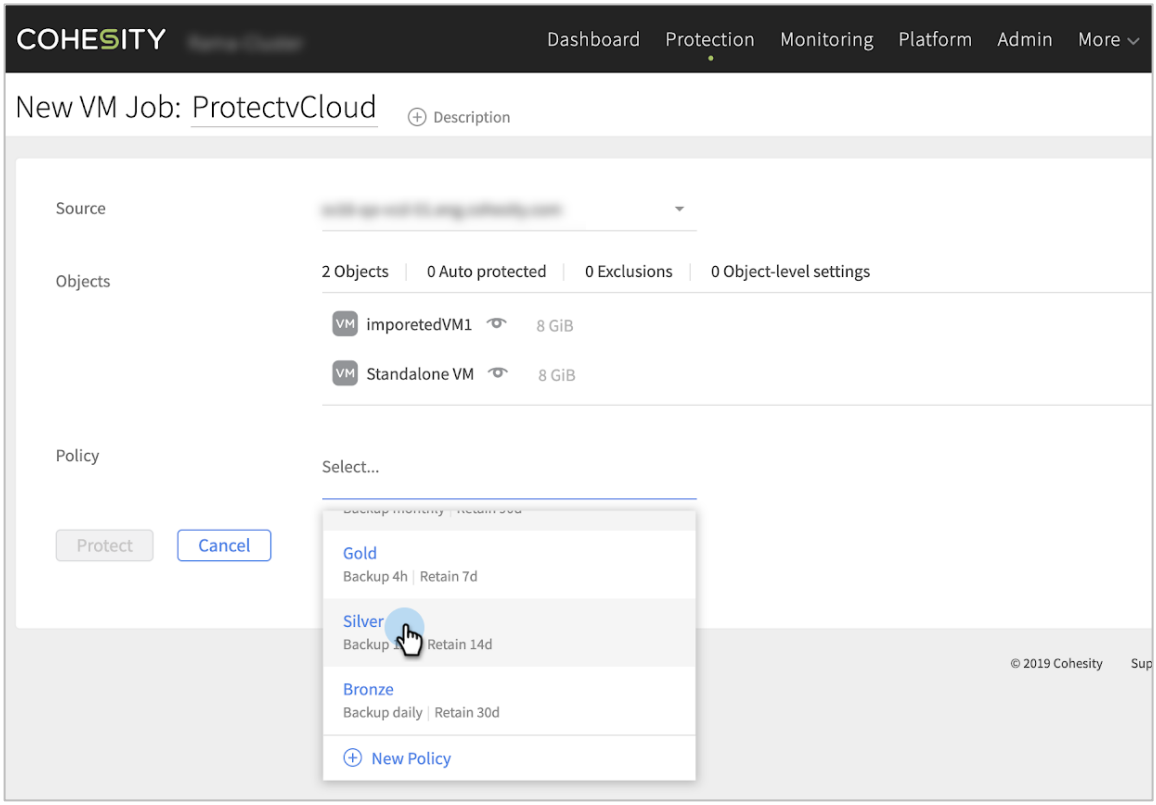
4. Select the vCD objects to protect, click the shield icon on the right to enable **Auto Protect**, and then click **Add**.



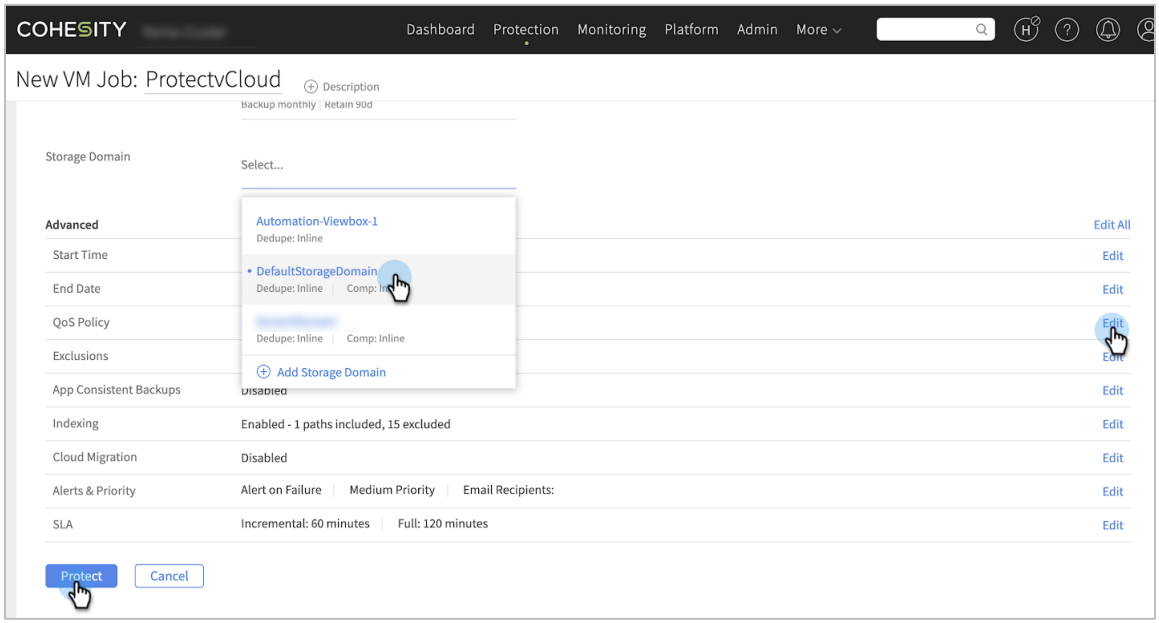
You can select entire vOrganizations, virtual data centers (vDCs), vApps, or individual VMs to protect. Selecting a parent object includes child objects as well.

When you also apply **Auto Protect** to any vCD object, Cohesity DataPlatform dynamically protects that object and any new child objects every time the Protection Job runs.

5. Select the Protection **Policy** to apply to your Protection Job. You can choose default policies – **Gold**, **Silver**, or **Bronze** – or a custom, user-generated policy. (If you prefer to create a custom policy, click **New Policy**.)



6. On the same screen, select a **Storage Domain**. If you need to change any of the Advanced settings, click **Edit** on the right. When you're done, click **Protect**.

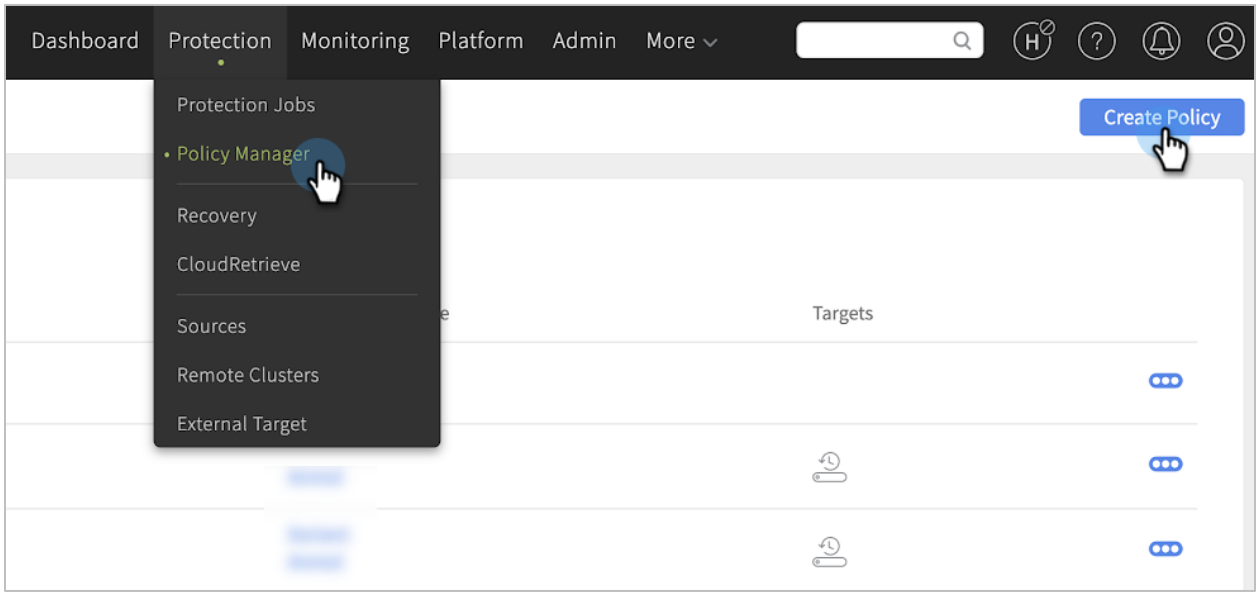


NOTE: See the complete list of **Advanced** settings for VM Protection Jobs in Appendix B.

5.2 Create a Custom Protection policy for vCloud Director

In addition to the predefined Protection Policies provided with Cohesity DataPlatform (Gold, Silver, or Bronze), you can also create custom Protection Policies that address the unique requirements of your organization.

In the definition of a new Protection Job, or when you select **Protection** > **Policy Manager** > **Create Policy**, you can create a new Protection Policy that includes additional workflow definitions, such as backup limits and retention time, replication, and archival.

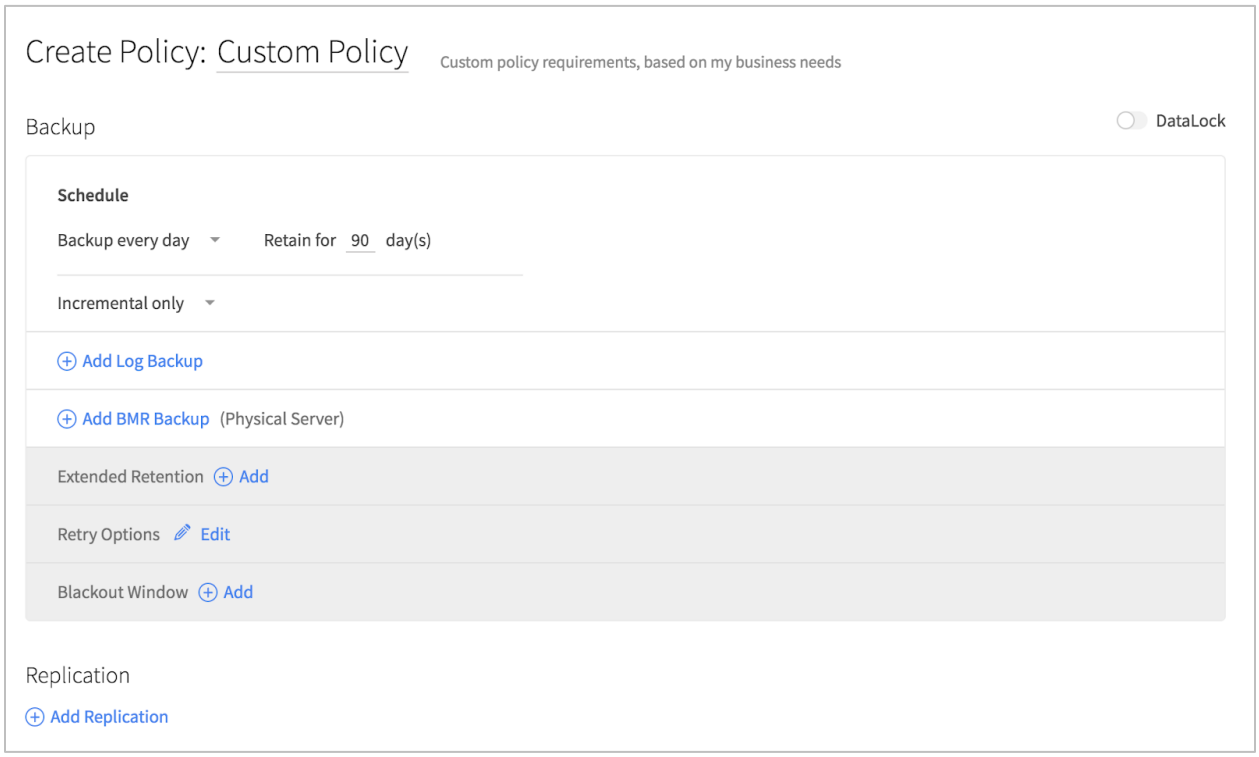


5.2.1 Define Advanced Backup Parameters

You can define the backup frequency by minute, hour, day, week, or month, and even the specific day and time you want backups to occur. As a corollary, the data retention period can also be defined.

Cohesity DataPlatform's granular control of backups allows you to define:

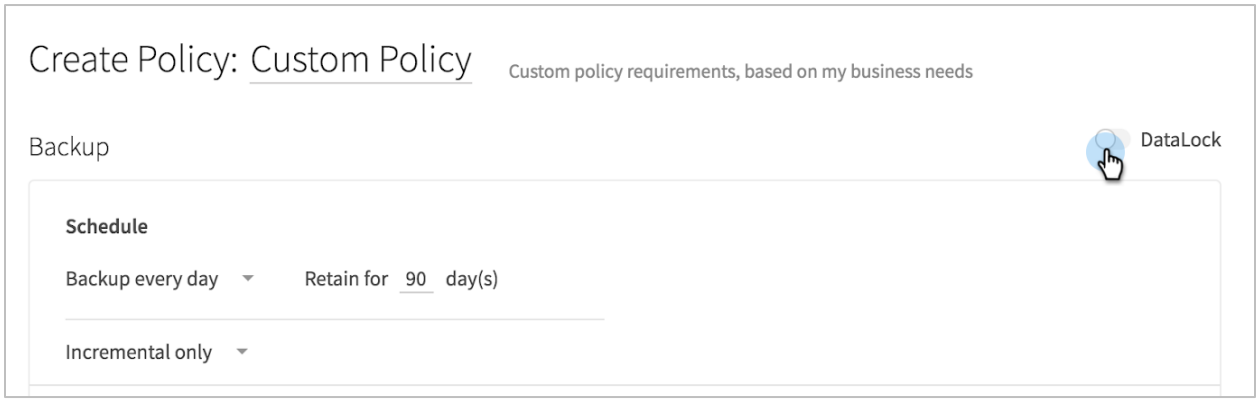
- The nature of the backup – incremental, or incremental with a full backup
- Blackout windows
- Extended retention options
- Retry options



5.2.2 Enhance Security with DataLock

In the same form, you can add a DataLock for compliance and regulatory requirements, to ensure that your protected data, including local backups, archives, and replication, cannot be modified until the DataLock expires. Once applied, a DataLocked Snapshot will be deleted only after its retention period expires.

A DataLock prevents all users, excluding those who have the Data Security role in Cohesity DataPlatform, from modifying or deleting any Snapshots that were generated by the Protection Jobs that use this policy. Only users with the Data Security role can add, modify, or remove a DataLock from a Policy.



5.2.3 Apply Legal Holds for Judicial Use Cases

Users who are assigned the Data Security role can put a legal hold on existing Snapshots (Protection Job runs), to preserve them for legal purposes. Once a legal hold is applied, the retention period is ignored, and the Snapshot is preserved until the legal hold is removed. Legal hold Snapshots can only be deleted by a user with the Data Security role.

NOTE: A legal hold can be added to both regular and DataLocked Snapshots.

You can add a legal hold to a Protection Job run or to individual objects in a Job run:

- If you add a legal hold to a Job Run, it applies to all the Snapshot objects that were backed up by that Job Run, and the legal hold is propagated to replicated and archived objects.
- If you add a legal hold only to selected objects in a Job Run, the legal hold is propagated to archived objects, but not to the replicated objects. You must manage the legal hold status on the remote replication cluster manually.

NOTE: A legal hold prevents Snapshots from being deleted until the legal hold is removed. Using a legal hold for long periods of time can result in the cluster running out of space.

To add or remove a legal hold from a Protection Job Run, see Adding a Legal Hold to a Snapshot in the online Help.

5.2.4 The Difference between Legal Hold and Datalock

While both legal hold and DataLock are features that empower the Data Security role in Cohesity DataPlatform to prevent backed up and archived data from being deleted, they differ in purpose and function.

Table 2: The Difference between Legal Hold and DataLock

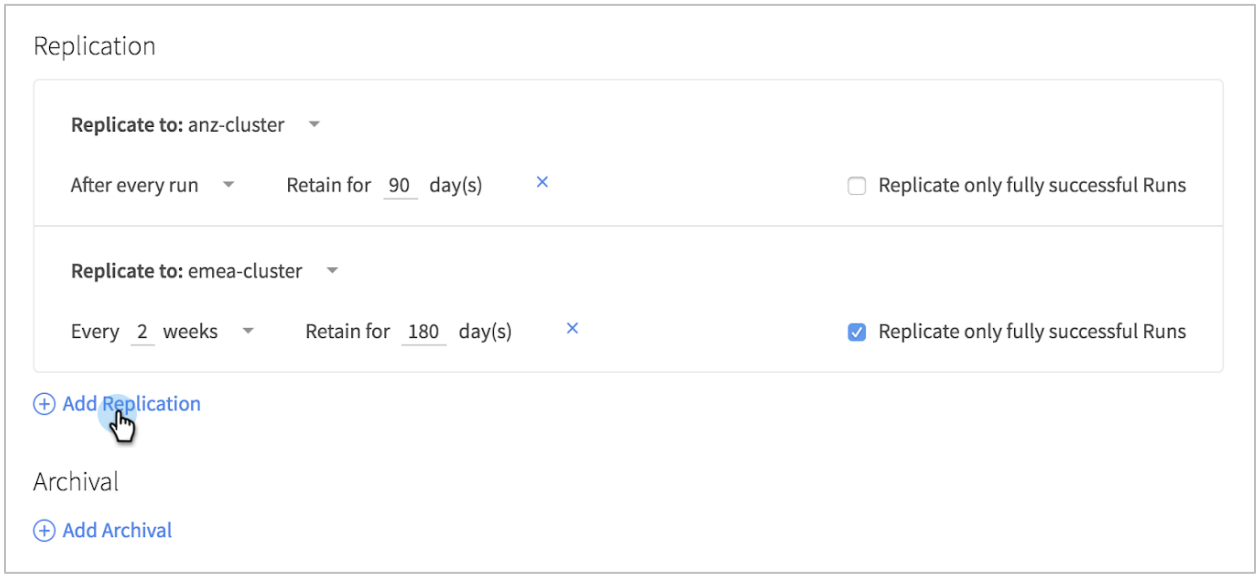
PURPOSE	LEGAL HOLD	DATALOCK
Business need	Reactive: Set on a specific Snapshot (i.e., Job run), usually prompted by legal requirements.	Planned: Set on all Job runs that use a Protection Policy with DataLock, usually for compliance.
Expiration period	No expiration. Removal managed by the user.	Defined in the Protection Policy.
Granularity	Set on individual Job runs and at the object level.	Applies to all Job runs of any Protection Jobs that use a Policy with DataLock.

PURPOSE	LEGAL HOLD	DATALOCK
Deletion	Can be deleted to recover storage space, but only by a user with the Data Security role.	Cannot be deleted before the DataLock expiration date, even by a user with the Data Security role.

5.2.5 Add Replication for Data Resiliency

Within a Protection Policy definition, you can configure the settings for replicating protected objects to remote clusters. You can schedule recurring replication, which further improves your data resiliency. You can select a replication target and replication frequency, and define the retention time. You can also add new remote replication targets and sources, allowing you to complete entire workflows without leaving the page you are on, enabling true single-pane management.

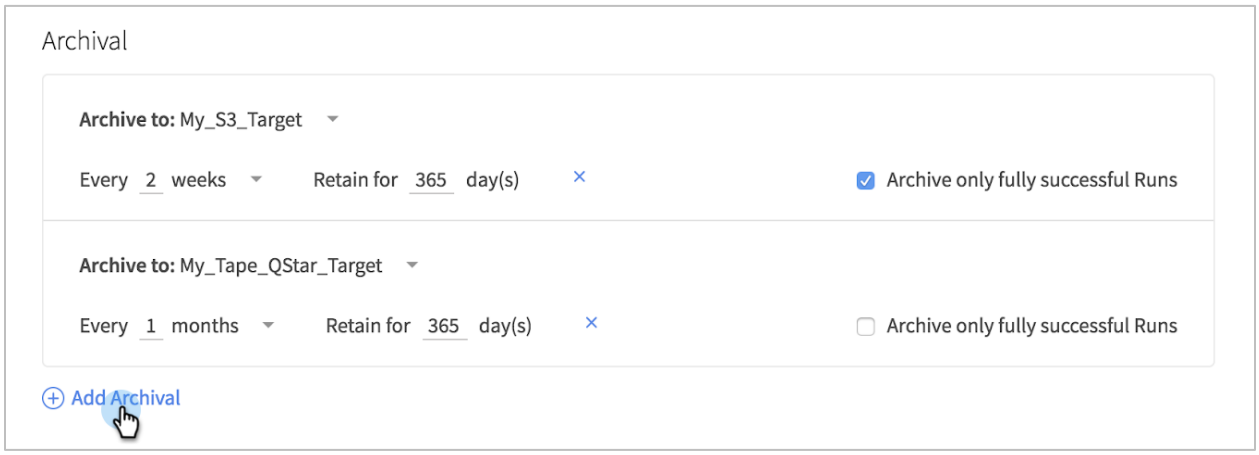
To apply replication to your Protection Policy, under **Replication** in the same page, click **Add Replication**.



5.2.6 Add Archival for Long-Term Retention

As part of a Protection Policy, you can define the archival target, frequency, and retention requirements. Custom data protection for VMware vCloud Director environments and tenant data is simple; archives of protected data can be sent to a gamut of targets, including targets in the cloud or on tape. This level of granularity and flexibility gives you data protection on your terms, working with your business requirements and infrastructure.

To define archival settings in your Protection Policy, under **Archival** in the same page, click **Add Archival**.


Archival
Archive to: My_S3_Target
Every 2 weeks
Retain for 365 day(s)
Archive only fully successful Runs
Archive to: My_Tape_QStar_Target
Every 1 months
Retain for 365 day(s)
Archive only fully successful Runs
Add Archival

6 Recover vCloud Director Objects

Cohesity DataPlatform provides granular recovery, enabling you to recover any organization, virtual data center (vDC), vApp, and individual VM in the vCloud Director environment.

6.1 Recover Files and Folders

You can search for and recover individual files and folders within virtual machines in VMware vCloud Director.

6.2 Recover VMs

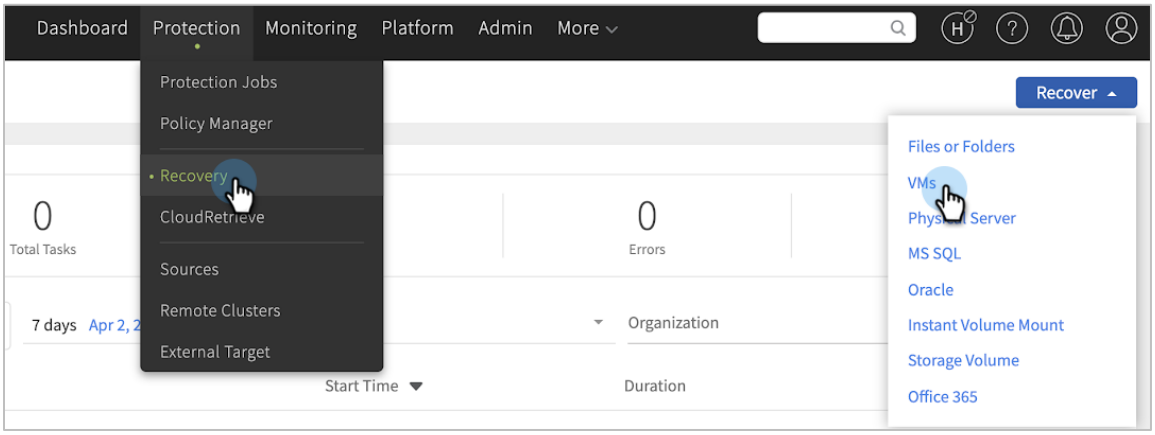
You can recover VMs to the same location, within a vApp, or virtual data center with the same configuration, providing greater data protection capabilities to multi-tenant organizations.

6.3 Recover vApps

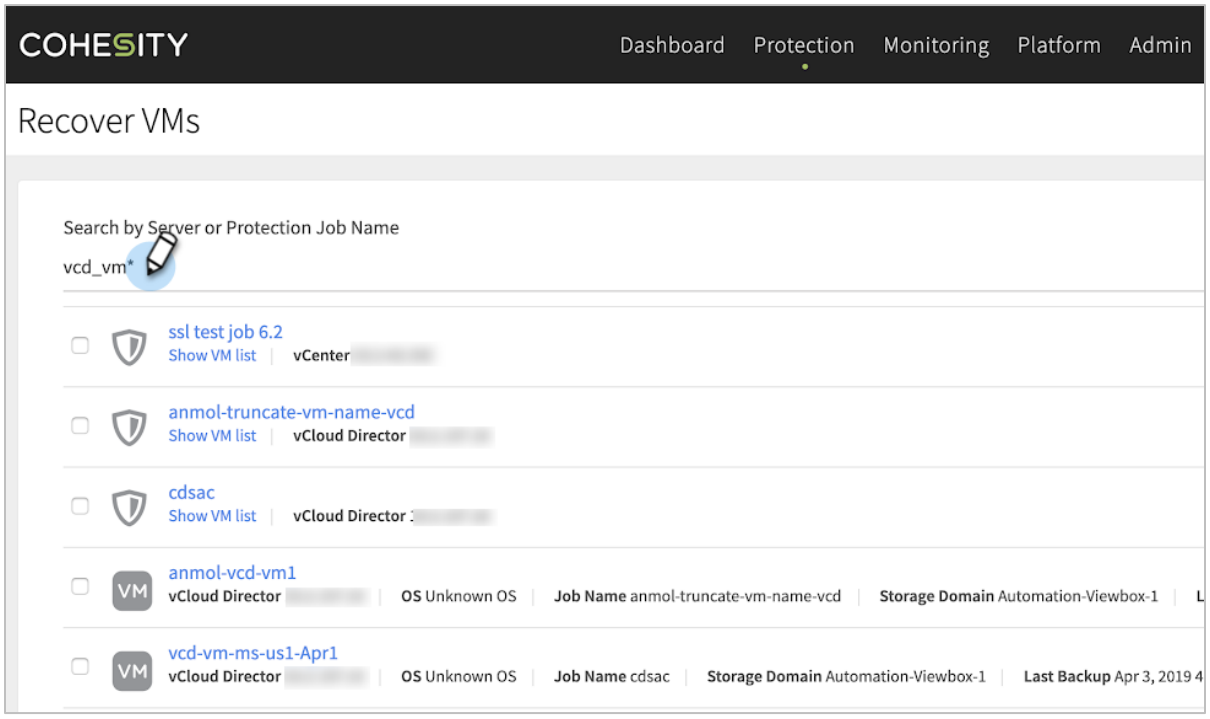
vApps can be backed up and recovered in a similar way, on-premises or across multi-clouds. Cohesity DataPlatform's integration with vCloud Director has been designed to support this level of flexibility as well as self-service backup and recovery.

To recover objects such as vApps, VMs, and files and folders:

1. Log in to DataPlatform and select **Protection** > **Recovery**. On the **Recovery** page, select **Recover** > **VMs**.

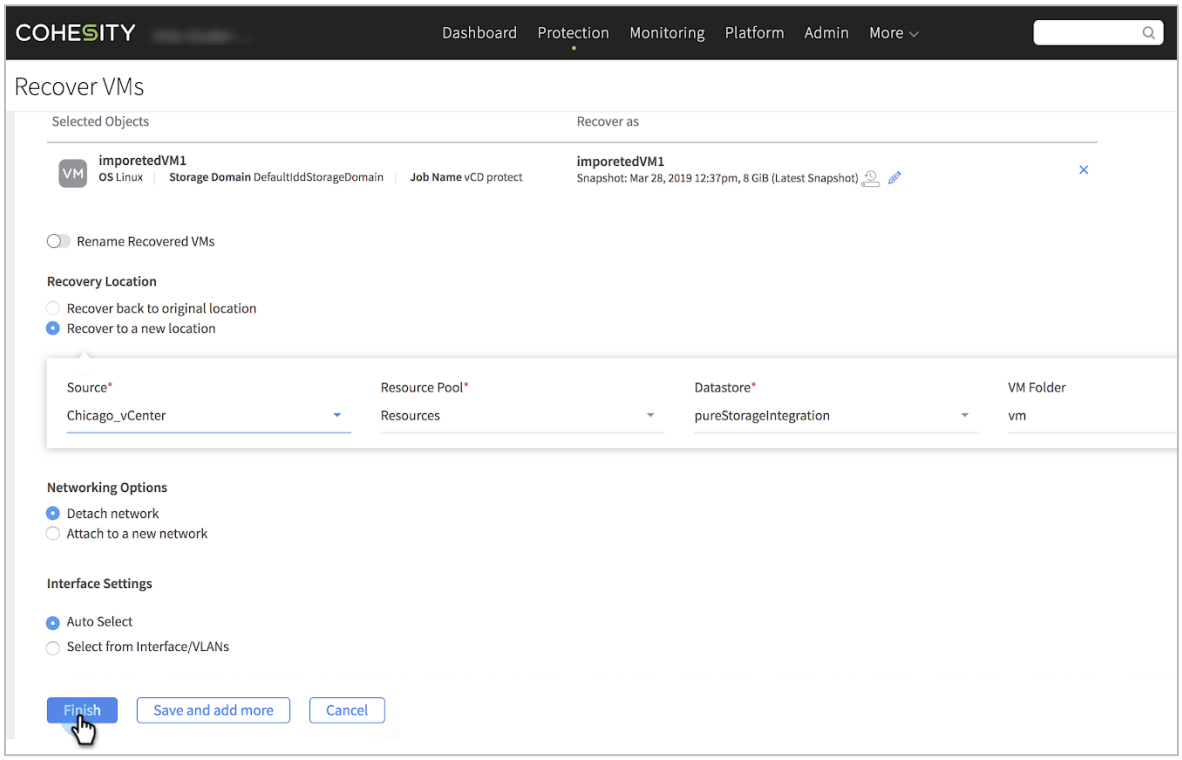


2. Type in a search query for the objects you want to recover.



NOTE: Cohesity DataPlatform supports wildcard characters to simplify management and recovery of vCloud Director objects.

3. Select **Recovery Location** (original or new), along with other networking options, and then click **Finish**.



6.4 Supported Recovery Locations

Table 3 describes the supported recovery locations for vCloud Director objects.

Table 3: Supported Recovery Locations

OBJECT	WORKFLOW	SUPPORTED RECOVERY LOCATIONS
VM	Backup	Original location, alternative vDC, alternative vApp
	Archival	
	Replication	

OBJECT	WORKFLOW	SUPPORTED RECOVERY LOCATIONS
vApp	Backup	Original location, alternative vDC
	Archival	
	Replication	
Files and Folders	Backup	Original location, alternative vDC, alternative vApp
	Archival	
	Replication	

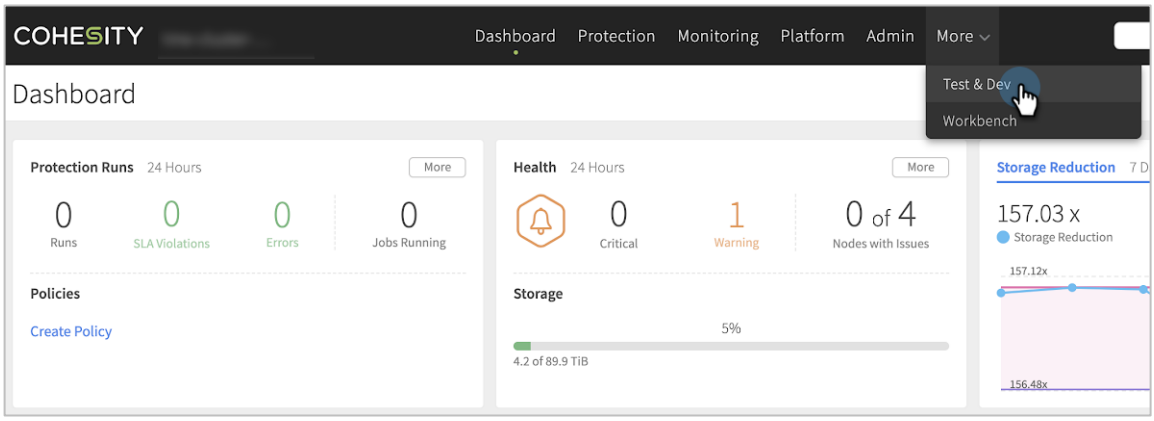
7 Clone vCloud Director Objects for Test and Dev

Cohesity DataPlatform is also a great platform for test and dev, promoting the use of your data, going beyond solely protecting it. In an organization with multiple tenants and different development efforts, copy data management can help lower development time significantly and bring self-service agility to test and development teams.

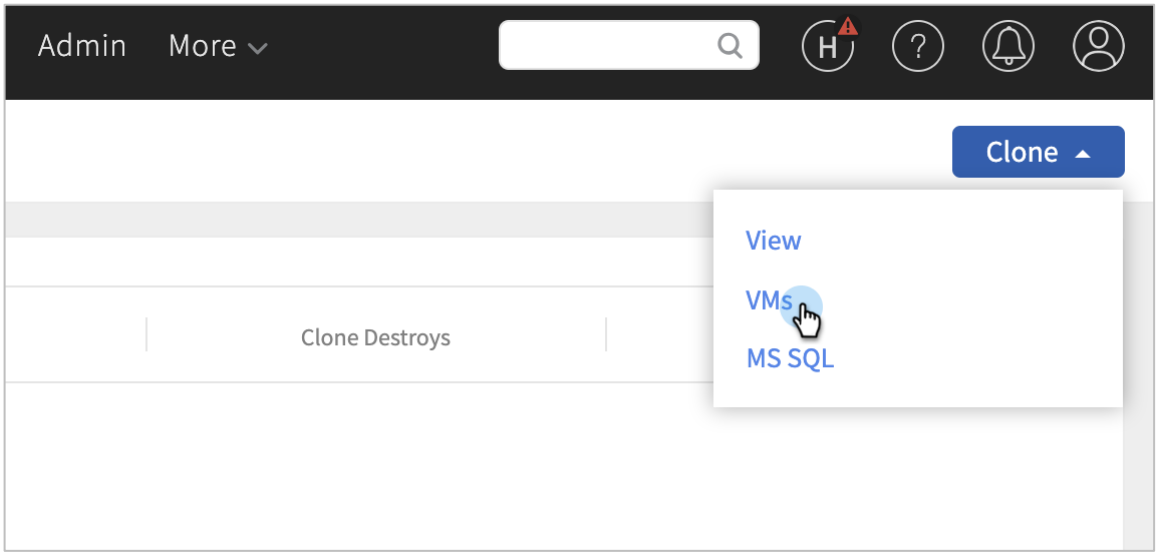
Cohesity DataPlatform allows you to create clones that are writable, supporting global deduplication for any new data written.

To clone protected VMs in your vCloud Director environment:

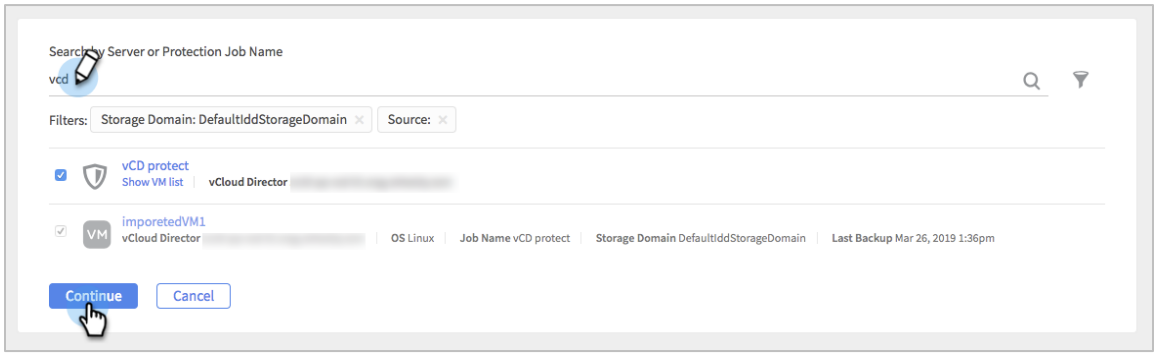
1. Log in to Cohesity DataPlatform.
2. Select **More** > **Test & Dev**.



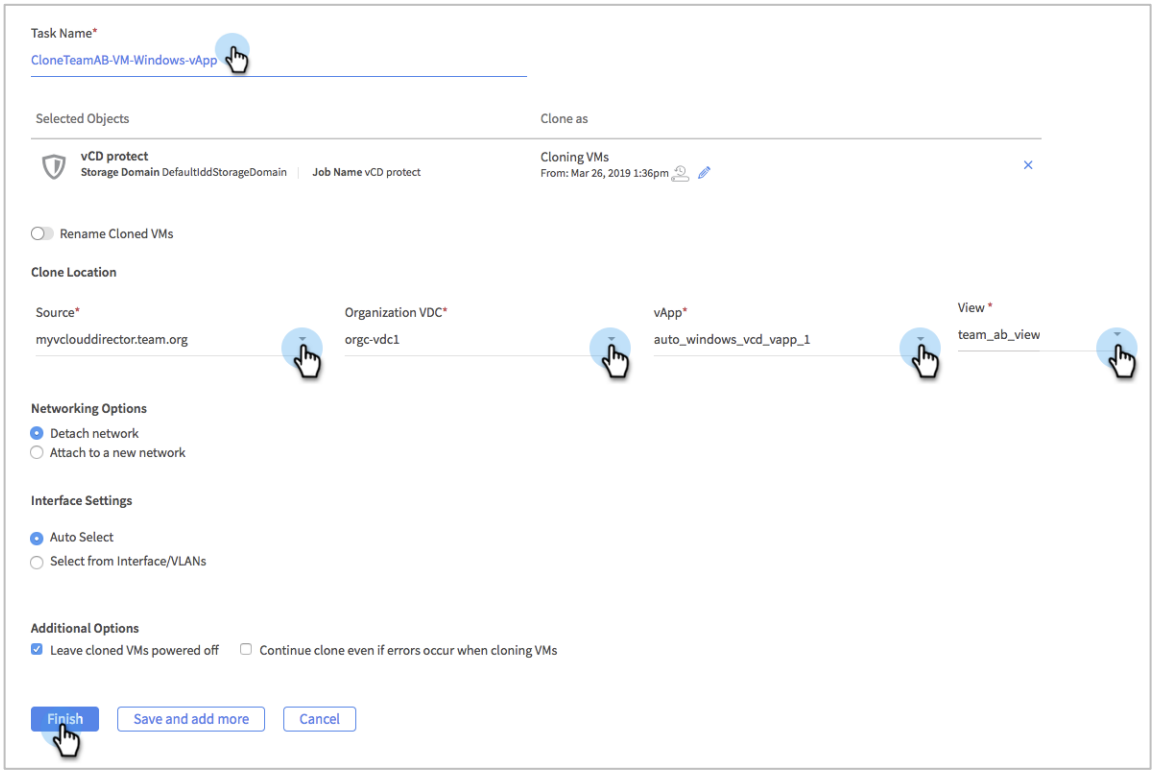
3. Click **Clone** > **VMs**.



4. Search for protected VMs by the VM name or the Protection Job name you specified.



5. Define **Task Name**, **Clone Location**, **Networking Options**, **Interface Settings**, and **Additional Options**, and then click **Finish**.



8 Use Archival and Replication for Disaster Recovery and Business Continuity

Data and application retention is critical to organizations that seek to prevent data loss and meet security, legal, compliance, disaster-recovery, and business-continuity requirements.

Cohesity DataPlatform provides two solutions for disaster recovery and business continuity:

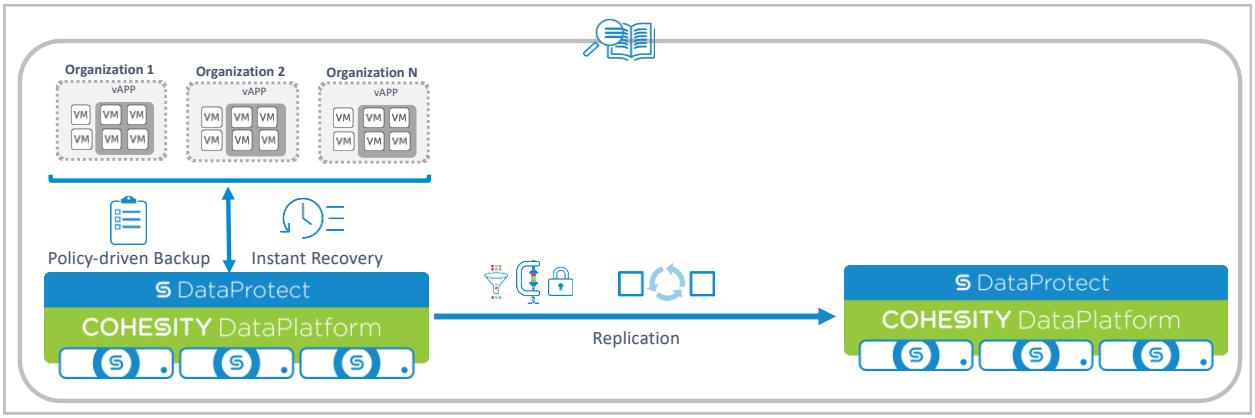
- Cloud Replication
- CloudArchive and Retrieval

8.1 Replicate to the Cloud for Cost-Effective Disaster Recovery

VMware vCloud Director administrators can take advantage of Cohesity replication for cost-effective disaster recovery (DR). Cohesity DataPlatform provides a policy-based data replication solution from the core to the cloud to the edge, from one cluster to another cluster in your DR site.

As part of replication, Cohesity DataPlatform always performs source-side deduplication and compression first and sends only the changed data over the network. In the event of the primary site becoming unavailable, application and backup admins can fall over to the DR site for backup and recovery of their data.

Figure 2: Replicate backups to other DataPlatform clusters for additional data resiliency

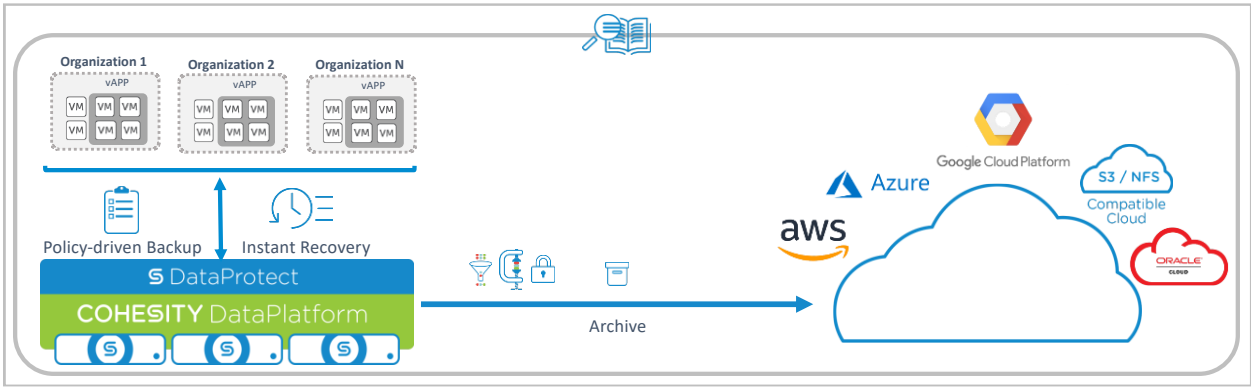


8.2 Use Cohesity CloudArchive and Retrieval for Long-Term Retention

The exponential growth of data volumes and the resulting IT management demands have prompted businesses to seek more cost-effective, reliable data storage and protection solutions. Cohesity DataPlatform provides a policy-based method to archive to public clouds (AWS, Azure, GCP), to any S3-compatible storage, tape, and/or to any NFS mount point. Cohesity CloudArchive offers a complete, self-contained copy of your backup, containing backup data, backup metadata, indexing data, and deduplication fingerprints.

VMware vCloud Director administrators can take advantage of Cohesity CloudArchive to address long-term data retention requirements. The archived data is efficiently transferred and stored by sending only deduplicated, compressed, incremental backups, thereby reducing network and storage utilization.

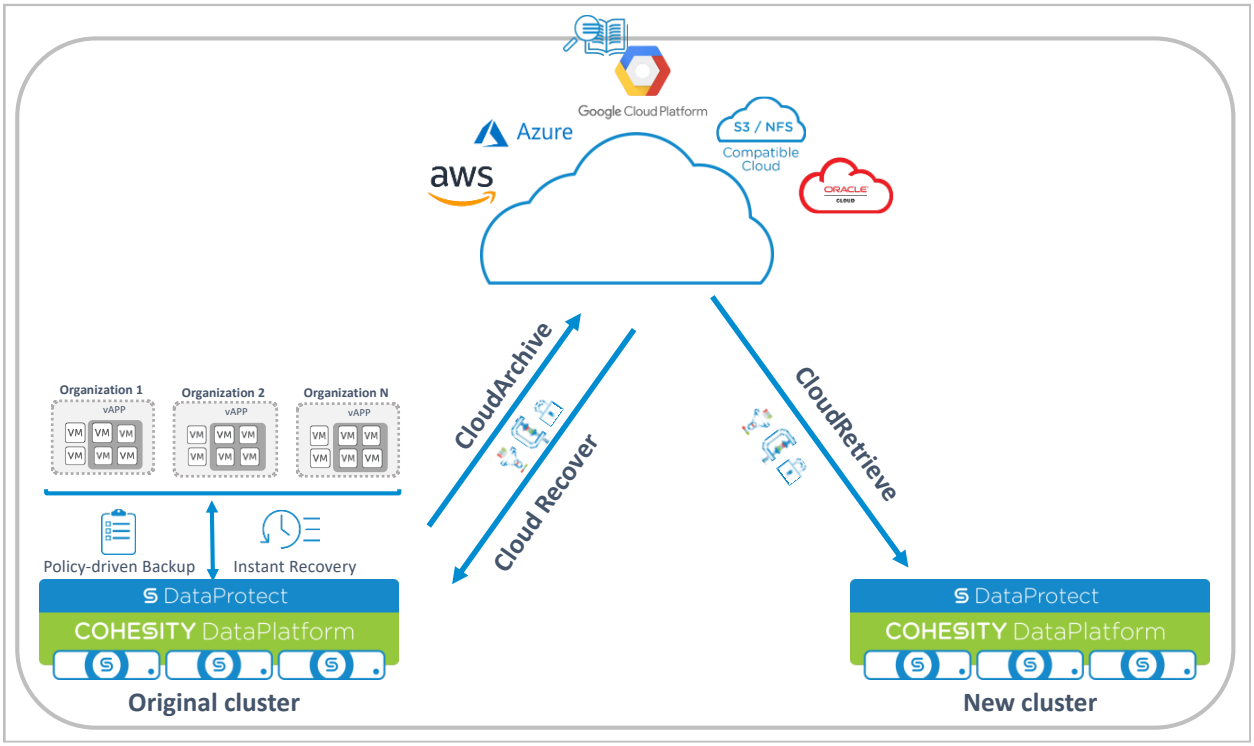
Figure 3: Leverage public cloud infrastructure for long-term data retention and archival requirements.



Once the data is archived, VMware vCloud Director administrators can also take advantage of the Cloud Recover and CloudRetrieve features:

- **Cloud Recover** to source cluster: Recover entire objects to your original cluster.
- **CloudRetrieve** to new cluster: Retrieve your previously archived data onto an entirely new cluster, as a cost-effective alternative for disaster recovery, geo-redundancy, and business continuity.

Figure 4: Cloud Recover to original cluster & CloudRetrieve to new cluster



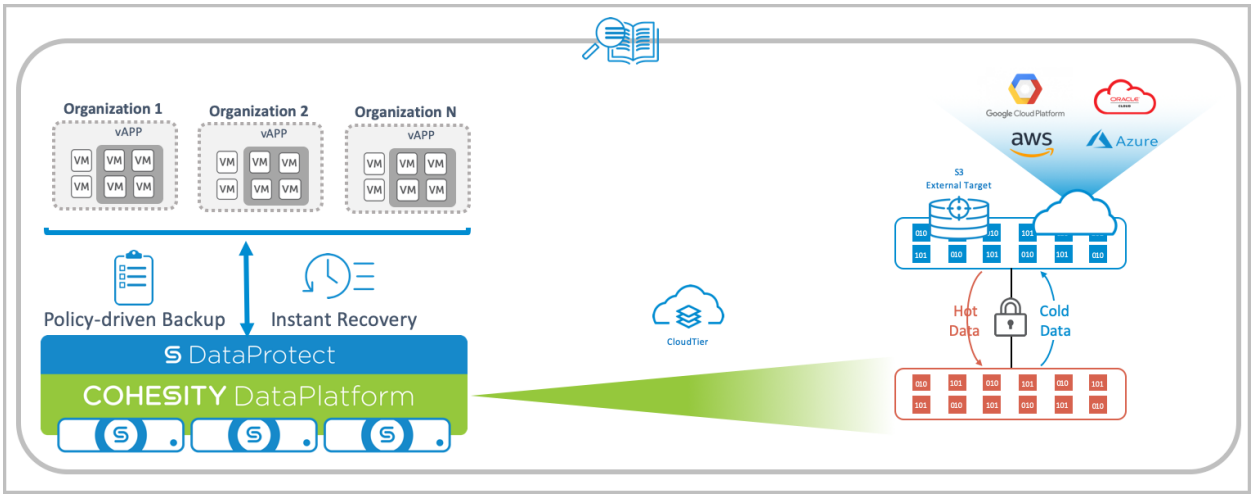
To learn more about CloudArchive, see the CloudArchive & CloudRetrieve Deployment & Recovery Guide.

9 Use CloudTier for Long-Term Retention and Reduced TCO

The performance, availability, and cost requirements of storing and accessing your data can change based on your business needs. Cohesity CloudTier allows you to move data to lower-cost storage for infrequently accessed data, reducing operating expenses and helping you meet compliance and access frequency requirements. Cohesity DataPlatform can automatically move data between different tiers.

Data can be down-tiered to external targets such as public cloud infrastructure providers (AWS, Azure, Google Cloud Platform) or any S3-compatible external target, with a policy threshold approach. Hot data in external targets can be up-tiered back to the Cohesity DataPlatform cluster.

Figure 5: Cohesity DataPlatform supports data tiering with a policy threshold approach



DataPlatform supports data tiering from HDDs to public cloud infrastructure. Tiering is based on policy, and includes the following thresholds:

- Storage Utilization
- Age of Data

When these configured thresholds are breached, data is tiered to the cloud. When tiered data becomes hot data, data is seamlessly tiered from cloud to the physical cluster without user intervention.

Following the paradigm upheld throughout by Cohesity DataPlatform, all tiered data is compressed, deduplicated, and encrypted.

10 Cohesity Extensions for VMware vCloud Director

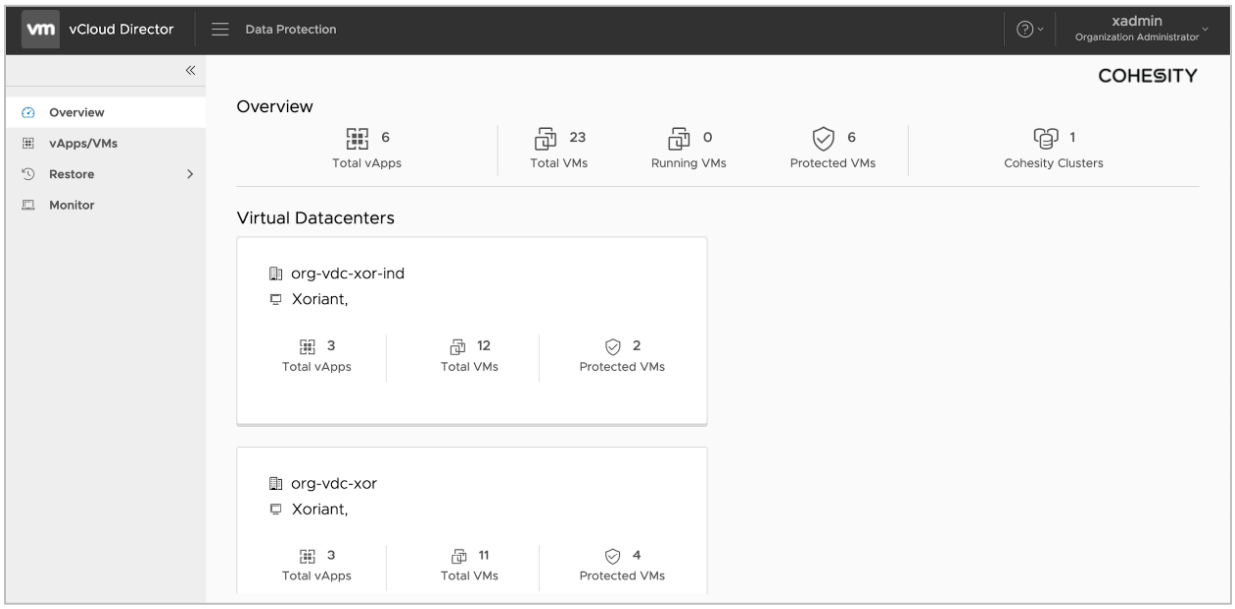
Cohesity DataPlatform provides deep integration with VMware vCloud Director and several multi-tenancy benefits, in both the Cohesity DataPlatform and vCloud Director UIs.

10.1 A Deeper Integration with VMware vCloud Director

In partnership with VMware, Cohesity brings the power of self-service to vCD tenants for backup and recovery with secure, native integration into the HTML UI. The experience is seamless for tenants because backup and recovery tasks, as well as IaaS, can take place in a single UI.

This complements Cohesity DataPlatform support for automated protection of vCD objects – including vOrgs, vDCs, vApps, and VMs – which safeguards enterprise data for single or multiple tenants. Each tenant environment remains secure with automated, role-based access controls.

Figure 6: Cohesity Extension for VMware vCloud Director shows protected objects at a glance



The Cohesity Extension for VMware vCloud Director leverages the power of the Cohesity REST API to deliver self-service backup and recovery at your fingertips.

10.2 Getting Started with Cohesity Extension for vCloud Director

Having an integrated backup and recovery service for VMware vCloud Director not only streamlines operations, but also provides a rich tenant experience that allows Cohesity and VMware Cloud Provider Program partners to offer differentiated services.

Cohesity Extension for VMware vCloud Director is available on GitHub. In addition, the extension is now available on the VMware Solution Exchange, a marketplace where customers can research, evaluate, and rate more than 2,500 solutions from VMware technology partners, systems integrators, and developers. The extension is available for VMware vCloud Director 9.5 and greater, along with Cohesity DataPlatform 6.2 and greater.

Learn more and get started with the extension on GitHub.

11 Conclusion

Cohesity DataPlatform solves data protection challenges for multi-tenant, self-service environments by delivering granular and flexible end-to-end data protection for vCloud Director.

Backup-as-a-Service and disaster-recovery-as-a-service are available to tenants without the need for backend orchestration. A native integration with VMware vCloud Director coupled with Cohesity DataPlatform features — such as our focus on multi-tenancy, flexibility, and seamless integration with public cloud infrastructure — solves many of the data protection needs of multi-tenant organizations. Cohesity DataPlatform reduces management time and cost for managed service providers, as well as for enterprise administrators who provide resources to multiple tenants.

12 Appendix A: Configuration Requirements

Verify that you meet the following requirements before proceeding with many of the workflows described:

- All vCenter networks should be available to all vCenter ESXi hosts in the cluster.
- Isolated networks require distributed switches.
- vCenter clusters in use with vCD must specify Fully Automated for vSphere DRS automation.
- All hosts in all clusters managed by vCD must be configured to require verified host certificates.
- Cohesity DataPlatform supports data protection for vCloud Director environments versions 9.0 and greater.
- The Cohesity Extension for vCloud Director supports vCloud Director 9.5 and greater.
- Registering as different administrators during source registration on Cohesity DataPlatform provides different levels of resource permissions:
  - Register as a vCD administrator for complete resource allocation and modification.
  - Register as a vOrg admin for resource allocation and modification within a particular vOrganization.

13 Appendix B: VM Protection Job Advanced Settings

Protection Jobs combine operational flexibility with the business requirements that are defined in a Protection Policy. See all the advanced VM Protection Job settings in Table 4 below.

Table 4: VM Protection Job Advanced Settings

FIELD	DESCRIPTION
Start Time	Available only if the selected Policy has a Backup frequency other than hourly. Indicates when the Job should run. The current time is displayed by default, but you can change it.
End Date (optional)	Toggle on End Date and select the date on which the Protection Job stops capturing Snapshots. A Job Run that starts prior to this date will run until completion even if it completes after this date.
QoS Policy	Select HDD or SSD. **Backup HDD**: The Cohesity Cluster writes the data directly to a HDD drive for this Protection Job. **Backup SSD**: The Cohesity Cluster writes the data directly to an SSD drive for this Protection Job. Only specify this policy if you need fast ingest speed for a small number of Protection Jobs. We recommend HDD (the default).

FIELD	DESCRIPTION
App Consistent Backups	Toggle **App-Consistent backups** for a Protection Job if you want the guest Operating Systems of all the VMs in the Job to be quiesced before Snapshots of these VMs are created. If this option is selected, the Cohesity Cluster makes a request to the VMware vSphere software to create a quiesced VM Snapshot by invoking VMware Tools (installed on the guest Operating Systems of the VM). The VMware Tools requests that applications on the guest OS quiesce their state so application-consistent Snapshots can be created. This quiescing of VMs prior to capturing Snapshots ensures the integrity of the data saved in the Snapshots. **App-Consistent backups** apply to VMs only. For physical servers, Windows is app-consistent by default and Linux is crash-consistent. If the **App-Consistent** backups toggle is on, then **Take a Crash Consistent** backup if unable to perform an **App Consistent backup** toggle is available. Toggle it on if you want the Cohesity Cluster to capture a Crash Consistent Snapshot if the Cohesity Cluster fails to capture an App-Consistent Snapshot. For example, the Cluster may be unable to perform an App-Consistent backup when VMware Tools is not installed on the VM, the VM is powered off, or the VM cannot be quiesced. With this option enabled, Cohesity DataPlatform will not capture a Snapshot unless the cluster is able to perform an app-consistent backup.
Indexing	Indexing is required for file recovery. The Cohesity Cluster will scan all the files in the Protection Job and create an internal index that can be used later by a Recover task to locate files by name. When creating a volume-based SQL Job, indexing is not turned on automatically. Cohesity recommends turning indexing on because indexing is required to restore .mdf, .ldf and .ndf files from the cloud.
Exclusions and Inclusions: Indexing	Everything is indexed by default. Toggle on Exclusions and Inclusions if you want to exclude or include locations. By creating exclusion and inclusion rules, you can limit the Protection Job to a specific set of files and directories and therefore minimize the disk space used to store the data.

FIELD	DESCRIPTION
Cloud Migration	Enable this option to support the Cloud Migration of VMs and vApps between hypervisors (such as vCenter) servers and Cloud Services for failover and failback. Cohesity agents must be installed on the Windows VMs prior to backing up the Snapshots on the on-premises Cohesity Cluster. Disaster Recovery using Cloud Migration is currently supported for Windows VMs backed up from a VMware vCenter Source. For more information, see Disaster Recovery of VMs using Cloud Edition in the online Help. After enabling Cloud Migration, you can download the Cohesity Agent directly from the Cohesity Dashboard.
Alerts	Select one or more of the following settings if you want Alerts to be created for the following triggers: **Success**: Create an Informational Alert when a Protection Job completes successfully. Emails are not sent when Informational Alerts are created. **Failure**: Create a Critical Alert if the Protection Job fails to complete. Emails are sent when Critical Alerts are created. **SLA Violation**: Create a Warning Alert if the Protection Job takes longer than the time period specified in the SLA field. Emails are sent when Warning Alerts are created.
Priority	Select a priority for the Protection Job execution. Cohesity supports concurrent backups, but if the number of Jobs exceeds the ability to process Jobs, they are executed in priority order: **High** first, then **Medium**, and **Low**.
Email Recipients	You can add an email address to a Protection Job to notify the email recipients when Alerts are triggered for the Job.
SLA	The Service-Level Agreement (SLA) defines how long the administrator expects a Job to run. **Incremental**: Enter the number of minutes you expect an incremental backup job run to complete. An incremental backup captures only the differences (changed blocks) since the last job run. **Full**: Enter the number of minutes you expect a full backup job run to complete. A full backup captures the entire object (all blocks).

For more information, see Add or Edit a Protection Job for Virtual Servers in the online Help.

14 Document Version History

VERSION	DATE	DOCUMENT HISTORY
0.9	April 2019	Preview release
1.0	May 2019	First full release
1.1	Sept 2019	Update

15 About the Authors

Srini Sekaran is a Product Marketing Manager at Cohesity, focusing on data protection.

Other essential contributors included:

- Adaikkappan Arumugam, Senior Manager, Technical Marketing, Solutions Engineering, and Tech Pubs
- Bart Abicht, Senior Technology Editor, Technical Marketing & Solutions Engineering
- Ramachandran Natesan, Member of Technical Staff, Engineering

16 Your Feedback

Was this document helpful? Send us your feedback!

ABOUT COHESITY

Cohesity makes your data work for you by consolidating secondary storage silos onto a hyperconverged, web-scale data platform that spans both private and public clouds. Enterprise customers begin by radically streamlining their backup and data protection, then converge file and object services, test/dev instances, and analytic functions to provide a global data store. Cohesity counts many Global 1000 companies and federal agencies among its rapidly growing customer base and was named to Forbes' "Next Billion-Dollar Startups 2017," LinkedIn's "Startups: The 50 Industry Disruptors You Need to Know Now," and CRN's "2017 Emerging Vendors in Storage" lists.

For more information, visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.