COHESITY

Cohesity Clean Room Solution for VMware

A comprehensive approach to Prepare for, Initiate, Investigate, and Remediate Cyber Incidents

Version 1.2

August 2025

Table of Contents

Figures

Tables

Introduction

The Cohesity Clean Room solution provides a trusted foundation that speeds incident response and supports investigations by SecOps teams while minimizing the risk of secondary attacks. Our modular design enables users to quickly set up an isolated environment, supporting the response and recovery process and allowing teams to mitigate threats faster.

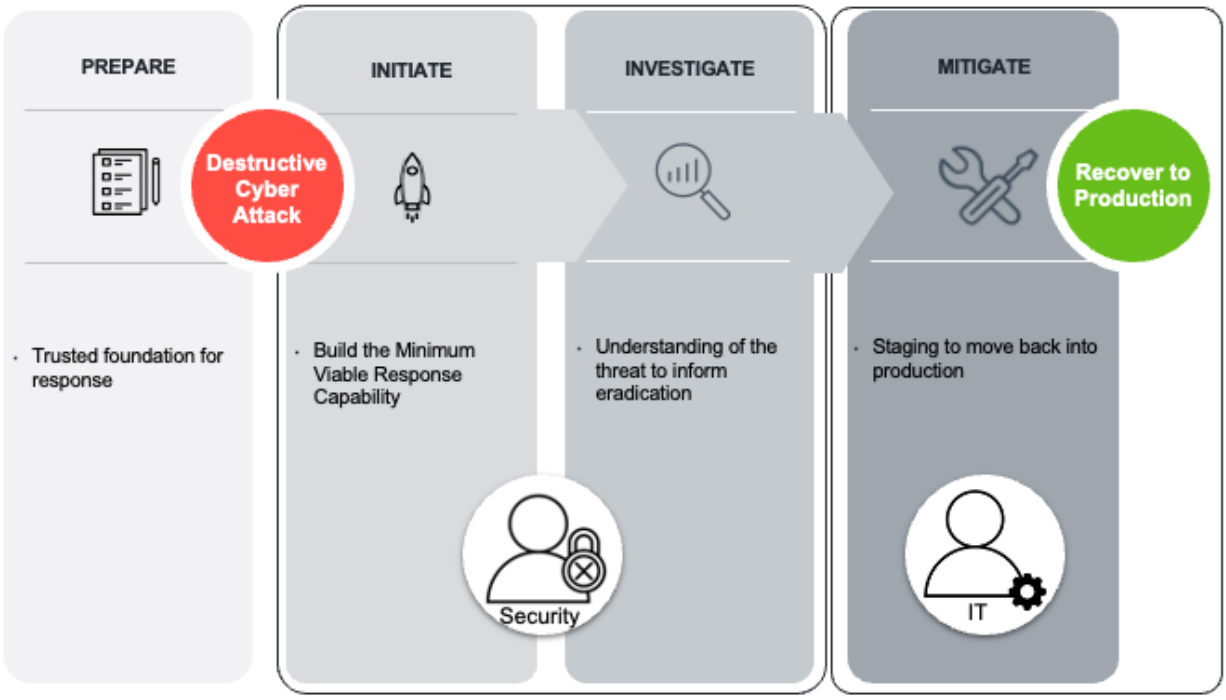
Our modular design begins with establishing a Minimum Viable Response Capability (MVRC). This trusted, known-good infrastructure can be established quickly to support the collaboration and communication of the response and recovery process. Restoring security operations tooling to a known good state that is used within an isolated environment helps the organization counter the multitude of evasion techniques adversaries use.

This guide will describe how to configure Cohesity Data Cloud to create the environment and take advantage of the native capabilities in the platform that support the Security Operations Team's needs in the clean room investigation.

Cohesity Clean Room Solution

Cohesity Clean Room solution uses a 4-stage holistic and structured framework (**Prepare, Initiate, Investigate, Mitigate)** for responding to and managing cyberattacks within a clean room or secure environment.

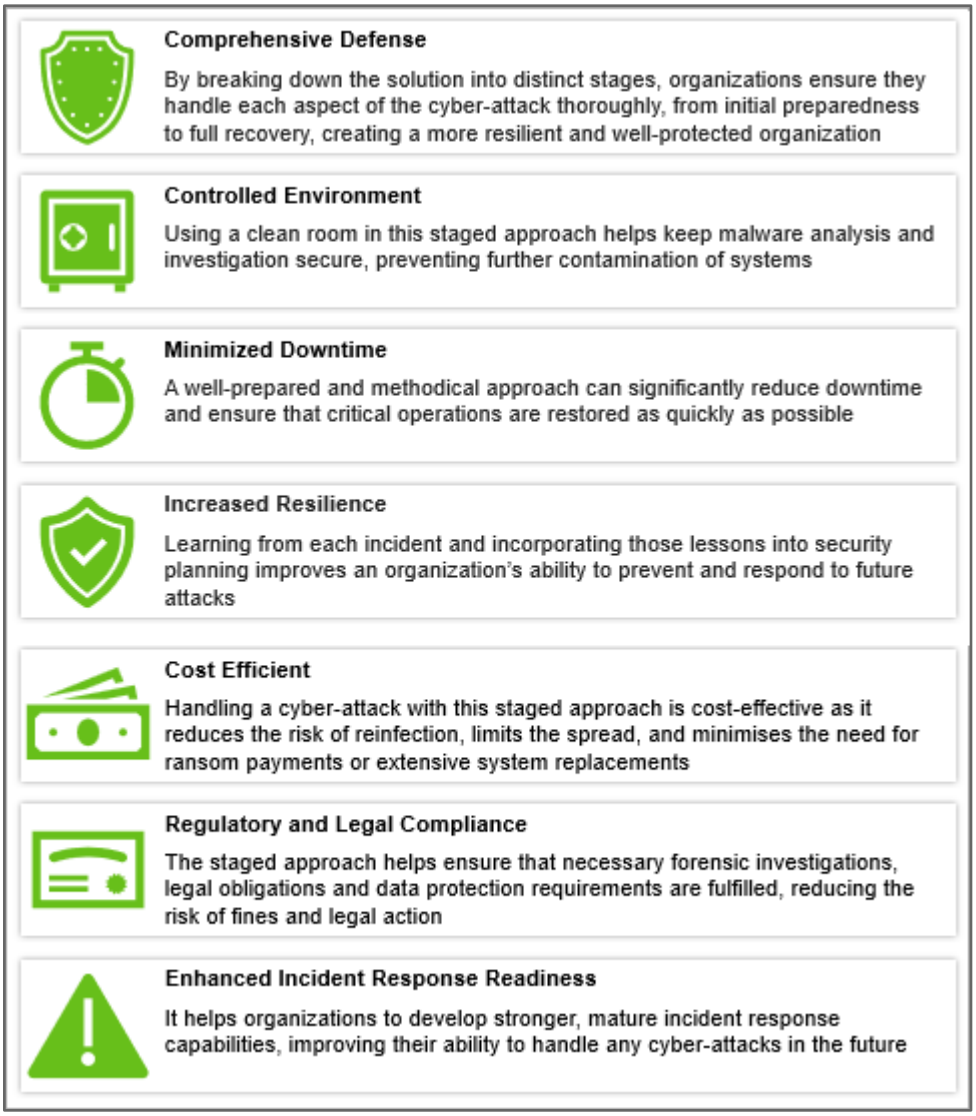
Figure 1: Cohesity Clean Room Solution



Each stage addresses key actions required to protect, detect, respond to, and recover from cyber incidents effectively.

1. **Prepare**: The **prepare** stage focuses on proactive measures taken to prevent cyberattacks and ensure you have trusted and available resources if one occurs.
2. **Initiate**: Once a cyberattack has been detected, the **initiate** stage involves triggering the response process to limit the damage, contain the threat, and preserve evidence for further investigation.
3. **Investigate**: The **investigate** stage focuses on understanding the scope and impact of the cyberattack, identifying its entry point, and assessing how deeply it has affected the systems.
4. **Mitigate**: The **mitigate** stage focuses on limiting the damage, recovering and testing in a staged environment, removing the malware from the network, and preventing further infections.

Benefits of Cohesity Staged Approach to Clean Room



Prepare

Establish Communication Protocols

A clear communication protocol in cyber recovery ensures efficient coordination, reduces confusion, and minimizes downtime. It defines roles, establishes communication channels, and outlines secure methods to protect information, enabling effective team collaboration throughout recovery.

The table provides an overview of some of the processes defined in the communication protocol.

Table 1: Establish Communication Protocols

Process	Purpose
Roles and Responsibilities	Ensures Accountability. For example, assign specific tasks to team members such as incident coordinators, IT responders, legal advisors, and executives who make decisions.
Communication Channels & Tools	Secure and Centralized Communication. For example, establish dedicated channels like Slack or Microsoft Teams for internal communication (VPN enabled) and ProtonMail for secure external updates.
Communication Plan	Effective Co-ordination. Create a structured plan using tools like Confluence or Google Docs, detailing who communicates what and when during recovery stages.
Regular Updates	Real-time Update. Utilize dashboards in ServiceNow or PagerDuty to inform all stakeholders of progress and next steps.

The 3-2-1+ Rule

The 3-2-1+ rule is part of the data protection disaster recovery (DR) strategy that involves creating at least three copies of an organization's data to be used as backups for operational resilience and business continuity. Two copies are stored on-site (but on different media), and one is stored off-site. Some customers may have more than three copies of their data to ensure they are well-prepared for potential cyberattacks.

In Cohesity data protection terms, the 3-2-1+ blueprint can be translated into three categories.

Table 2: The 3-2-1+ Rule

Type	Description	Topology
Mission Critical	A deployment topology with four or more copies. ***Highly Recommended***.	• Backup, dual Replication, and Archive • Backup, Replication, and dual Archive • Backup, dual Replication, and dual Archive
Enhanced	A deployment topology with three copies.	• Backup, Replication, and Archive • Backup and Dual Replication
Basic	A deployment topology with two or fewer copies.	• Backup • Backup and Archive • Backup and Replication

For more details on topology, refer to the Modern Data security and management topologies white paper.

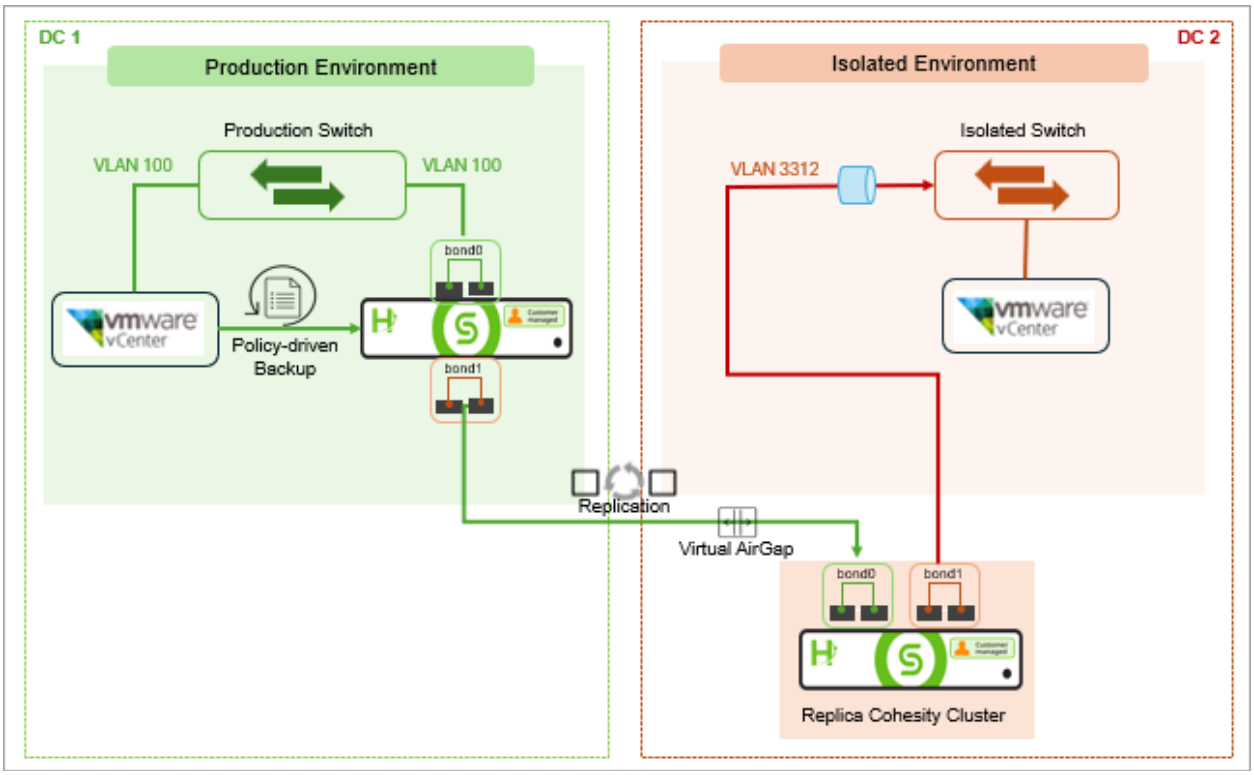
Cohesity Cluster Hardening and Best Practices

The Cohesity Platform helps ensure that data can be restored during a cyberattack and helps maintain business continuity by offering a reliable method to recover compromised or corrupted systems. Security hardening of the Cohesity Platform is essential as it minimizes vulnerabilities that attackers can exploit, thus protecting sensitive data and helping ensure the system's integrity. For more details on hardening your Cohesity cluster, refer to the Cohesity Data Cloud security hardening best practice guide.

Network Isolation

Network isolation is a crucial phase in data recovery for forensics and mitigation. It involves segmenting the network to ensure the isolated environment is completely disconnected from the production network. This can be achieved through physical segmentation using a dedicated network switch or logical segmentation using VLAN. The Cohesity cluster supports physical and logical network segmentation. The diagram below exemplifies how a VMware environment and Cohesity cluster are configured on an isolated network. Refer to the Create Isolated VLAN on Cohesity Cluster section to create an isolated VLAN on the Cohesity cluster.

Figure 2: Cohesity Clean Room Network Isolation



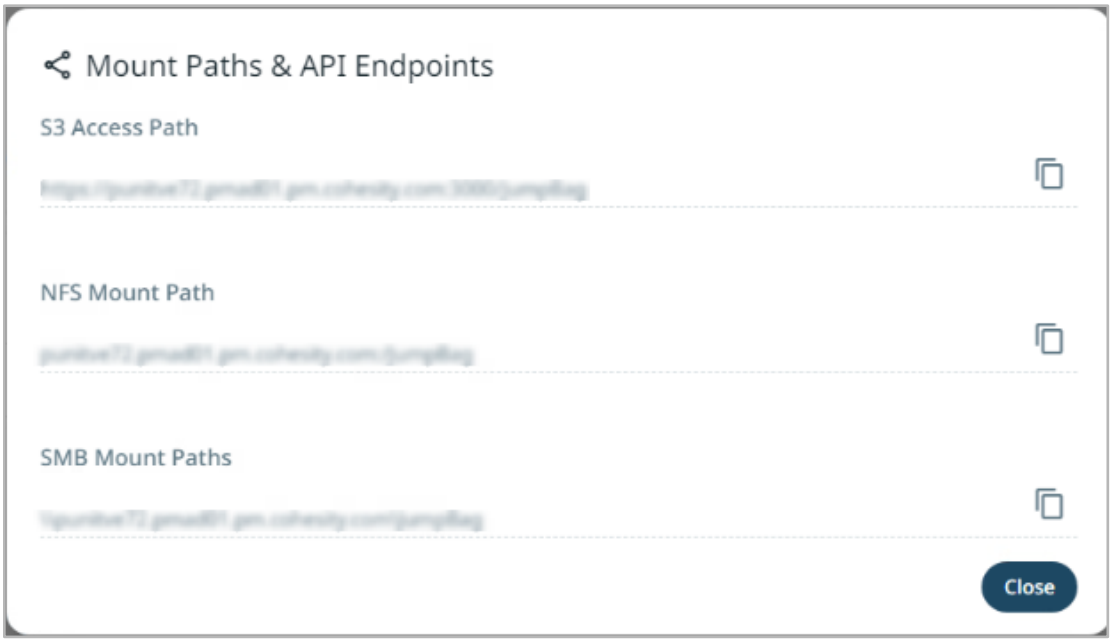
The networking designs vary from every customer deployment. Cohesity platform is designed and architecture to support various common network deployments. For more information, refer to Optimal Networking Designs with Cohesity and Cohesity Cluster Networking Quick Start guide.

Digital Jump Bag™

A Digital Jump Bag™ is a software repository to store critical workloads' ISO, software, configuration files, documentation templates, etc. In a cyberattack, the primary concern is how to regain trust in your setup/infrastructure. It's crucial to have access to vital data, such as golden copies and software, which should be stored in a secure vaulted location. This is necessary for rebuilding the infrastructure in an isolated environment and getting your dial tone workloads up and running, including Active Directory, DNS, security tools, contact list, recovery procedures, and more.

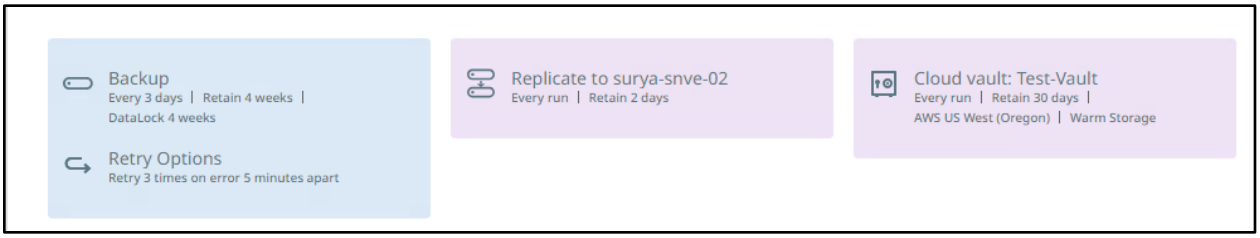
With Cohesity, you can create a Digital Jump Bag™ using SmartFiles View with data lock and object lock enabled. The view can be accessed using SMB, NFS, and S3 protocols. Furthermore, you can secure the Digital Jump Bag™ using Cohesity's policy-based replication and secure vaulting (FortKnox).

During the investigation phase, building a secure Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Domain Name System (DNS) infrastructure may slow down your response time to an attack. Cohesity provides a secure solution with local authentication and supports three access protocols: NFS, SMB, and S3, for SmartFiles View. Additionally, it enables mixed protocol access, allowing you to create a SmartFiles View using SMB and access it through the NFS protocol. Based on the severity of the attack, you can access the Cohesity SmartFiles view either directly from the cluster or through an out-of-band method managed via the Helios control plane.



Create Digital Jump Bag™

Customers can create the Digital Jump Bag™ and put all the data software repositories in the Cohesity SmartFiles view. Cohesity recommends you protect the Digital Jump Bag™ with DataLock, replicate, and vault your Digital Jump Bag™. Below is an example of a protection policy for the Digital Jump Bag™.



The following are the few key advantages of using the SmartFiles Views:

1. The file-level DataLock feature has WORM functionality on the live file system.
2. With SmartFiles Views, you can configure auditing and alerting to gain complete control and empowerment over your system's security.
3. Customers can compare different versions faster as you can present the SmartFiles View Quickly.
4. It's easy to configure the SmartFiles view, which is faster than fetching the information/data from the VM.
5. The common scenario for an attack on Windows is an attack on the Windows kernel. Cohesity SmartFiles views are presented in a secure way, which prevents bad actors from making modifications.

Cohesity SmartFiles View

Customers can configure the Jump bag using the SmartFiles view and write the data using any NAS protocol. For the jump bag, you must consider following Cohesity recommended approach below via Cohesity cluster UI and Helios:

1. Use SmartFiles file-level DataLock feature(WORM)
2. Protect and replicate the view to one or both
   a. Secondary Cluster
   b. FortKnox

In the case of the S3 protocol, leverage features like versioning and Object lock. The document describes creating and accessing the SmartFiles Views via NFS, SMB, and S3.

Digital Jump Bag™ Components

According to Digital Forensics and Incident Response (DFIR), a Digital Jump Bag™ is a portable collection of essential tools, equipment, and documents investigators carry to respond quickly and effectively to cybersecurity incidents. The components of a jump bag should be chosen based on the organization's specific needs, industry, and regulatory requirements. Refer to this blog to understand more about what components should be in the Digital Jump Bag™.

Hardware and Software Requirements

Table 3: Hardware and Software Requirements

Category	Components	Prerequisites	Comments
Cohesity	Cluster	Minimum: 3-Node physical cluster Latest LTS	This Cohesity Cluster can be either the primary cluster or a replication cluster, from which users can mount and retrieve the Digital Jump Bag™.
	SmartFile View	Forensic View	A Data Locked Evidence Collection View.
		Datastore view (optional)	Cohesity SmartFiles View is required if the user plans to use Cohesity as a datastore for ESXi.
	Cohesity Data Cloud Connectivity (Helios)	Yes	Claim the Cohesity clusters to Cohesity Data Cloud.
Infrastructure	Physical Server	For ESXi and vSphere	Physical server for installing ESXi and vSphere.
		Forensic Workstation	Physical server for Forensic workstation running either Windows or Linux. **Note**: This Physical Server can likely be a laptop.
	Dial Tone Apps	DNS, Mail servers, Phone communications, IAMs, Active Directory	
	Security Tools	Logging Tools, TIP, Forensic Tools etc.	

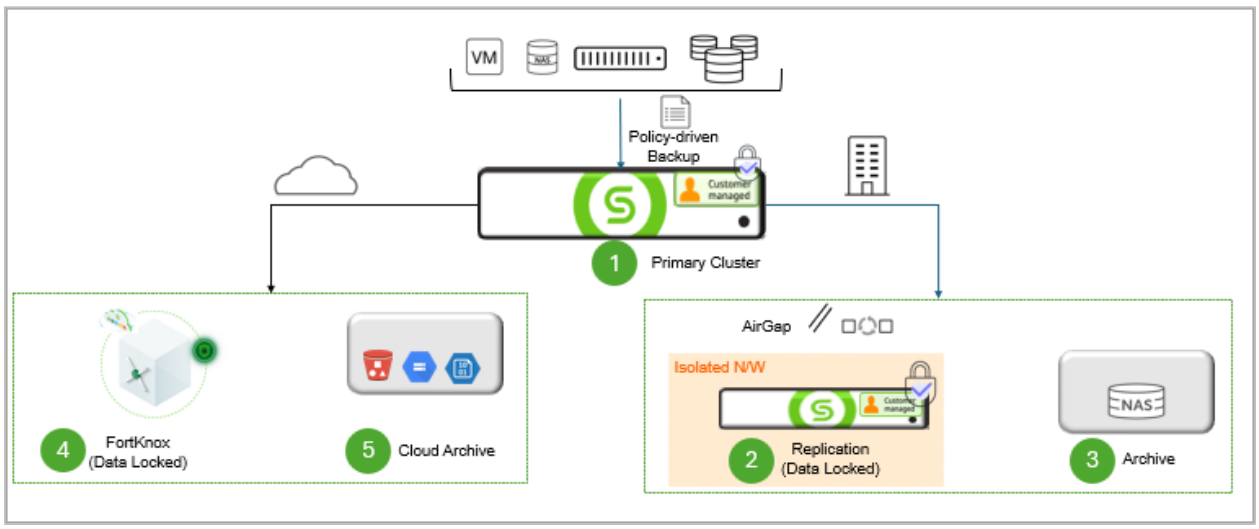
Category	Components	Prerequisites	Comments
Network	VLAN	Create an Isolated Network for Clean Room	
	Cohesity Cluster Access	Cohesity Cluster has a tunnel to Clean Room	
	Network Routers & Switches	Install Routers and switches inside Clean Room	
	Firewall	Configure Firewall	

Design Decisions

After setting up an isolated environment and obtaining the necessary ISO/Golden images from the Digital Jump Bag™ to construct the infrastructure components, the next crucial step is to identify the source from which to retrieve the data/snapshots for forensic analysis in the clean room and for mitigation in the staging room. Below is the Cohesity blueprint outlining the formats of your data.

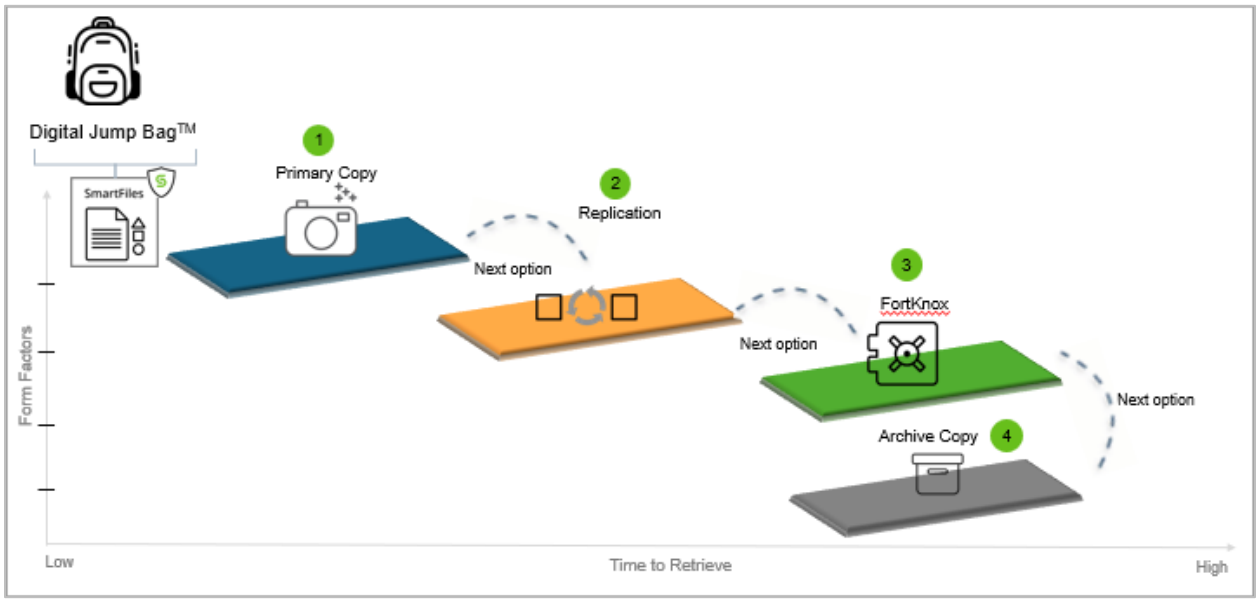
Table 4: Cohesity Topology and Form Factors

Location	Form Factors
Customer Managed On-Premise Locations / Data Centers	• Primary Cluster • Isolated Replication Cluster • NAS Archive
Cloud	• FortKnox • Cloud Archive



Cohesity can recover data from any form factor, with recovery methods varying based on the selected form factor. The high-level overview of the Cohesity blueprint and time to retrieval is as follows. You will find more details in the upcoming sections to help you choose the right recovery method.

Figure 3: Digital Jump Bag™ Retrieval Strategies



Initiate: Launch a Minimum Viable Response Capability (MVRC)

In cyber recovery scenarios, establishing a Minimum Viable Response Capability (MVRC) is essential for organizations to swiftly and effectively address security incidents. MVRC encompasses the critical tools and processes necessary to contain breaches, restore essential operations, and minimize downtime. By implementing an MVRC, businesses can ensure a prompt response, prioritize actions, and maintain basic operational continuity during attacks. Additionally, MVRC provides a foundational framework for incident response teams to efficiently manage the situation, ensuring a prepared and proactive stance in the cyber recovery process.

In this section, we will outline the essential steps to launch a Minimum Viable Response Capability (MVRC). The process includes:

1. Connecting the Cohesity Cluster to an Isolated VLAN
2. Retrieving and Mounting the Digital Jump Bag™
3. Configuring Routers and Firewalls
4. Installing Hypervisors
5. Setting Up Dial Tone Applications
6. Establishing Communication Protocols

Connecting a Cohesity Cluster to an Isolated VLAN

To initiate the clean room deployment, the first step is to build the network between the Cohesity cluster and the clean room. You have to first tag the isolated network switch to the clean room network. This can be accomplished through physical segmentation with a dedicated network switch or logical segmentation using VLANs.

If you follow the VLAN approach, the next step is to create the clean room network VLAN on the Cohesity cluster. If not, you should ensure the Cohesity cluster can communicate with the clean room isolated network. This section offers guidance on the configuration steps for implementing logical network segmentation with VLANs.

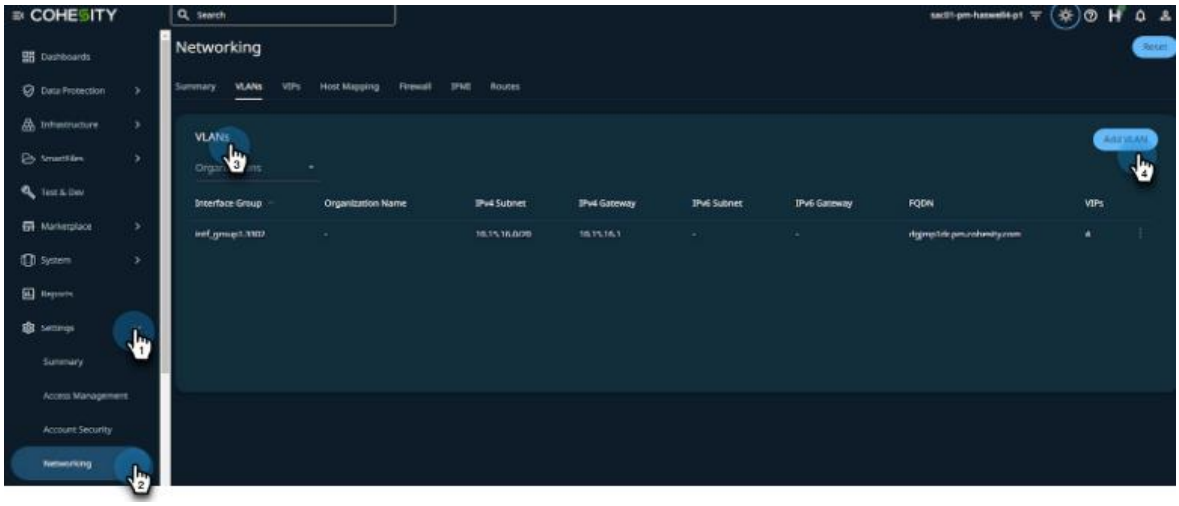
Create Isolated VLAN on Cohesity Cluster

After setting up the isolated infrastructure, the next step is to configure the VLAN on the replica or isolated replica Cohesity cluster to recover the data for forensics and mitigation. Follow the steps below to configure the VLAN on a Cohesity cluster.

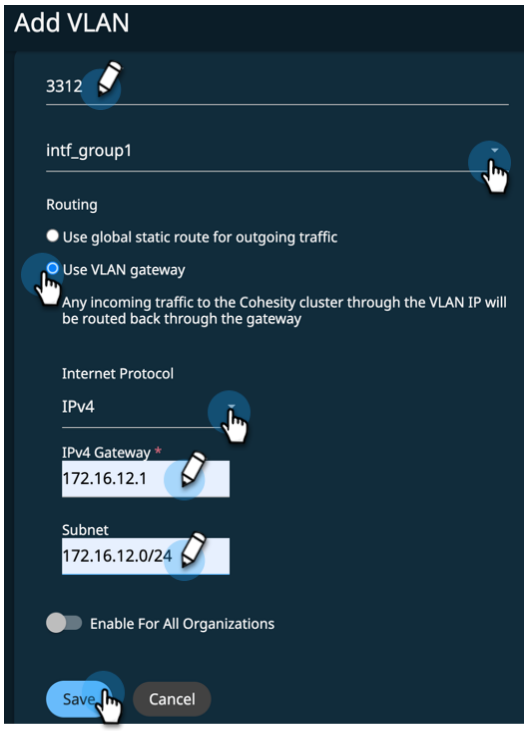
NOTE: You must create 2 VLANs for the clean room and staging room, respectively.

Follow the steps below to add the clean room VLAN and staging room VLAN.

1. Log in to the Cohesity cluster using your credentials.
2. Navigate to **Settings > Networking**. On the right pane, click **VLANs > Add VLAN**.



3. Enter the following fields:
   a. Add **VLAN ID.**
   b. **Select the interface group name** (if you have a dedicated secondary network, select intf_group2).
   c. **Routing**: Choose a global static route or VLAN gateway.
   d. (Optional) If the VLAN gateway is selected, choose the **Internet Protocol, IP Gateway, and Subnet**.
4. Click **Save**.



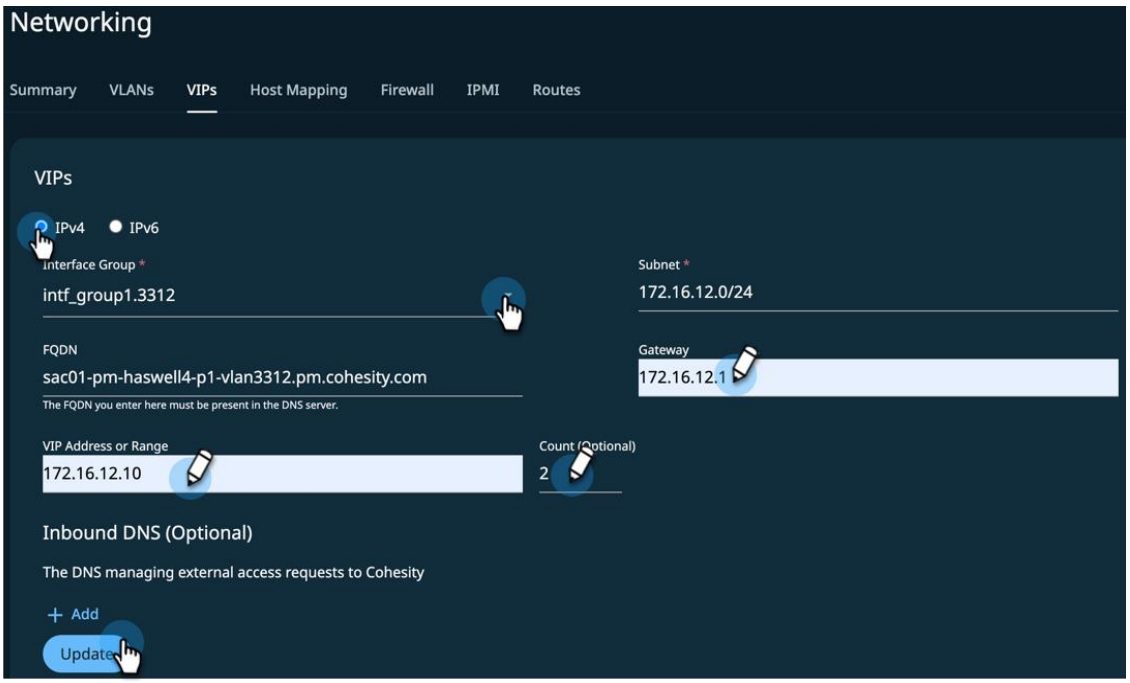
Create VIPs for the Isolated VLAN

After creating the isolated VLAN, you must create Virtual IP addresses (VIPs) for the VLAN interface.

NOTE: You must configure VIPs for both clean room and staging room VLAN.

Follow the below steps to create VIPs.

1. Log in to the Cohesity cluster using your credentials.
2. Navigate to **Settings** > **Networking** > **VIPs**.
3. Configure the following fields:
   a. Select **IPv4** or **IPv6.**
   b. Select **Interface Group** (This is the VLAN interface group created in Create Isolated VLAN on Cohesity Cluster. E.g., intf_group1.3312).
   c. Subnet and FQDN will be automatically populated.
   d. **Gateway**
   e. **VIP Address or Range**
   f. **Count** (recommend would be as per the number of nodes on the cluster)
   g. (Optional) Inbound DNS
4. Click **Update**.



NOTE: After creating an isolated VLAN and VIPs on the Cohesity cluster, ensure the Cohesity cluster VLAN VIP is pingable from the isolated environment. For example, ping the Cohesity VLAN VIP from a VM inside the isolated environment.

Digital Jump Bag™: Retrieval Strategies and Mounting to Forensic Workstation

After establishing connectivity to the clean room isolated network, the next step is to access the data from the jump bag. You can do this by mounting the Cohesity SmartFiles view on hosts. There are three methods to retrieve the data from the jump bag to the clean room isolated network.

1. Primary Cluster
2. Isolated Replica Cluster
3. FortKnox

Table 5: Digital Jump Bag™ Retrieval Strategies

Cluster	Description	Use case
Primary Cluster	Cohesity Cluster in DC or production location.	You can use the jump bag in case of a Security Drill or when you trust your production environment.
Isolated Replica Cluster	Cohesity Cluster on the DR site has the replicated copy.	You can use this cluster when the primary cluster is down or you want to retrieve the jump bag data on the DR site.
FortKnox	Cohesity-secured vaulting solution.	If you lose access to both the primary and replicated copies, you can retrieve the data from FortKnox to any standby Cohesity cluster.

Primary Cluster

Why should you use the primary cluster to retrieve the data? There are two reasons:

1. If your security team trusts the Cohesity primary cluster because they are completely aware of Cohesity's immutable system and its core security measures, they may consider it secure from compromise.
2. Proactively performing a clean room drill and using the primary cluster.

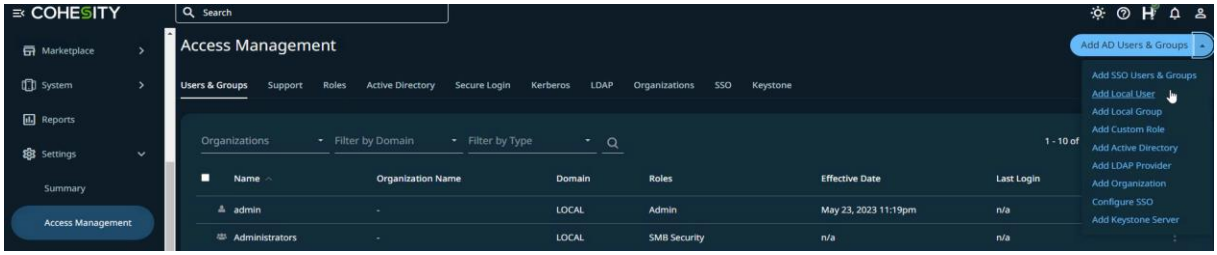
You can use the primary Cohesity cluster to retrieve the jump bag. As mentioned in sections Create Isolated VLAN on Cohesity Cluster and Create VIPs for the Isolated VLAN you need to create the isolated VLAN on the Cohesity cluster. Once networking is in place, mount the jump bag using the following process.

1. Retrieve the mount path location from the Cohesity View. The following will be the location to access the View:
    a. SMB: \\Isolated_VLAN_VIP\View Name
    b. NFS: Isolated_VLAN_VIP:/View Name
    c. S3: https://Isolated_VLAN_VIP:3000/View Name

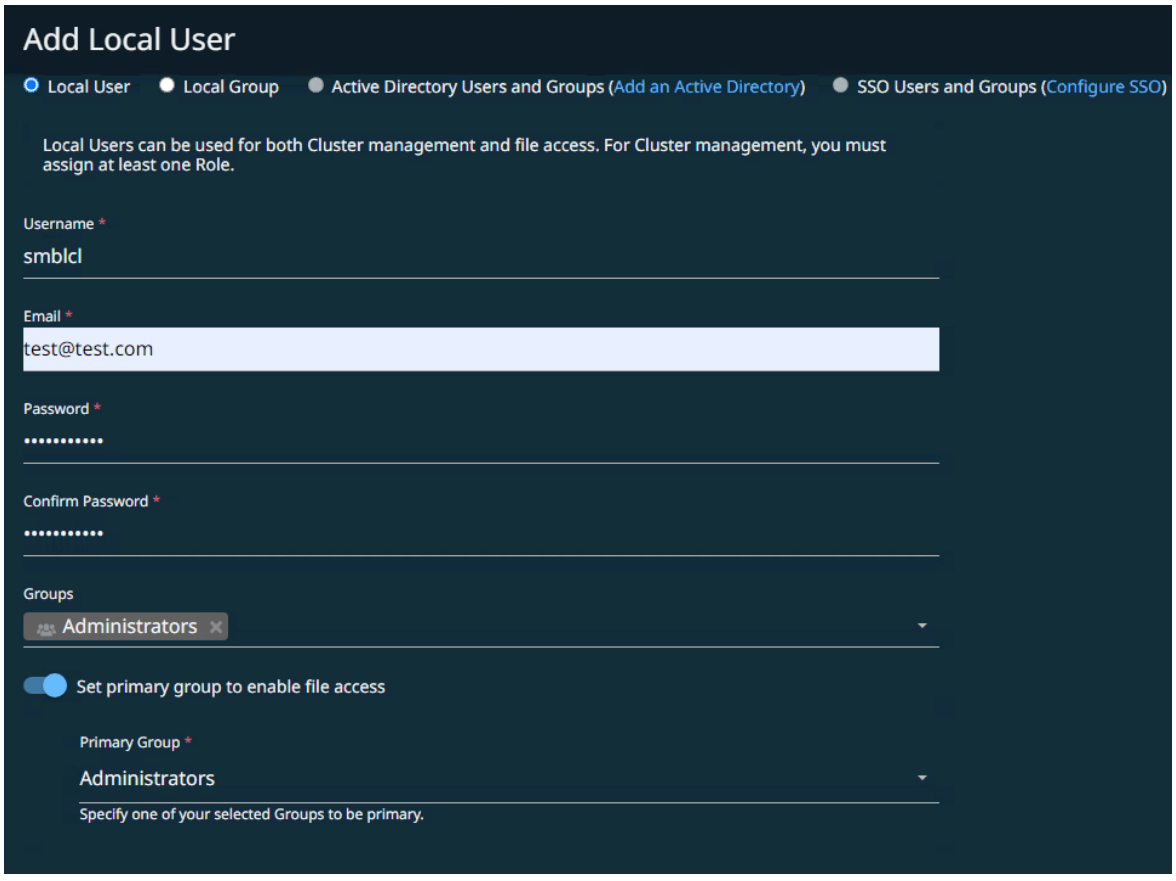
2. You need to access the SMB and NFS View to mount it. Here, we have two scenarios.
    a. **Scenario 1:** Your AD/LDAP is serving the authentication service, and in this case, you can mount the View with the standard process.
    b. **Scenario 2**: In this case, you lost AD/LDAP and do not have any authentication service. Cohesity will allow you to access the View locally without AD/LDAP.

SMB View

1. Log in to the Cohesity cluster and navigate to the **UI** > **Settings** > **Access Management** > **Add AD Users and Groups**. Click **Add Local User**.



2. Enter the information and select the group. Enable the option "**Set primary group to enable file access**." Click **Add**.



3. On the Windows server, you can use the command line as follows:

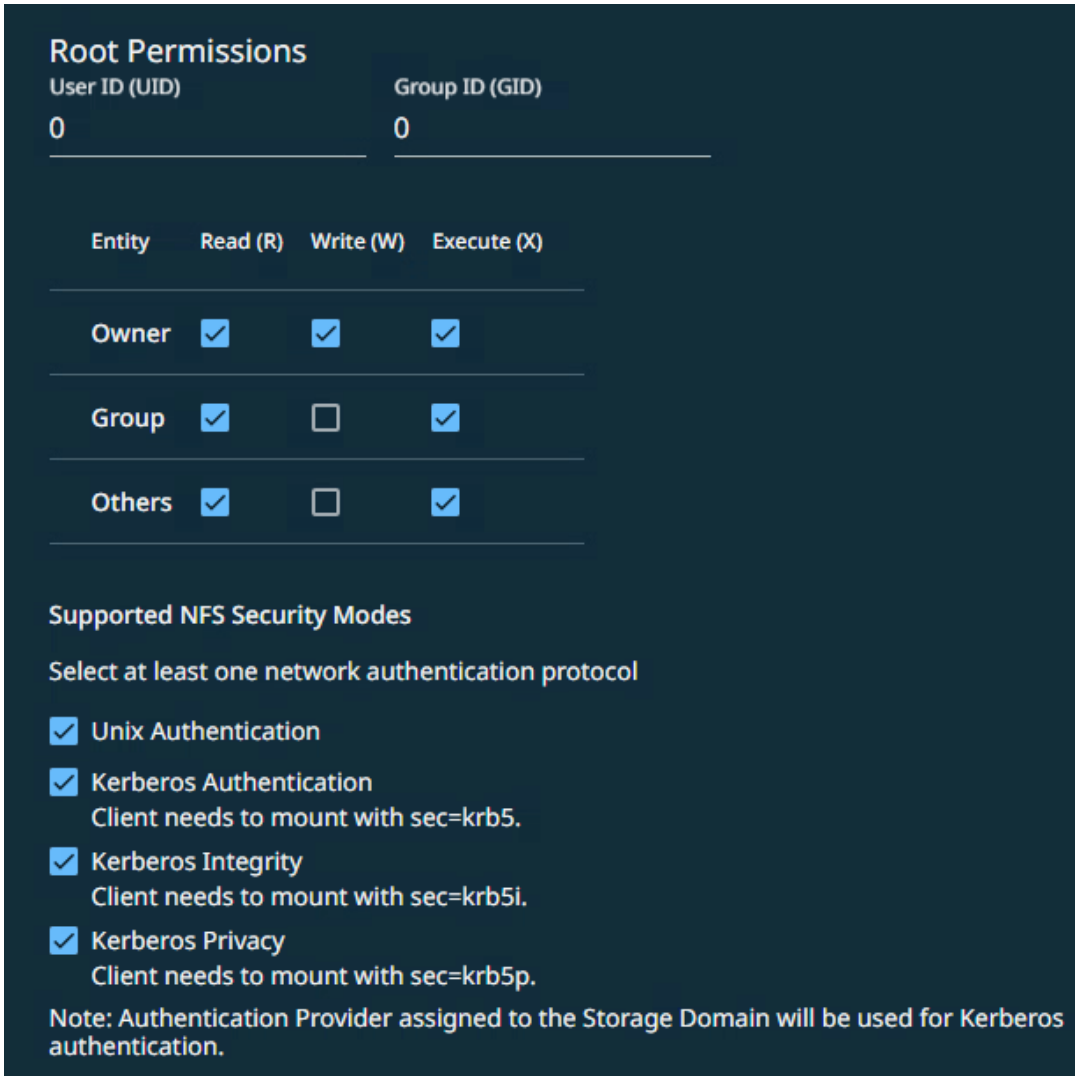
```
net use * \\<cluster_name>\<viewname> /user:cohesity\<username>
<password>

Example:
net use * \\my_cluster\myview /user:cohesity\johndoe <password>
```

If you want to use Windows Explorer, you have to enter the user and its credentials by using Cohesity as a domain name. Example: Cohesity\username.

NFS View

1. To mount the NFS view, you should enable root mounting on the edit section of the View.



2. Mount the view by using the mount command.

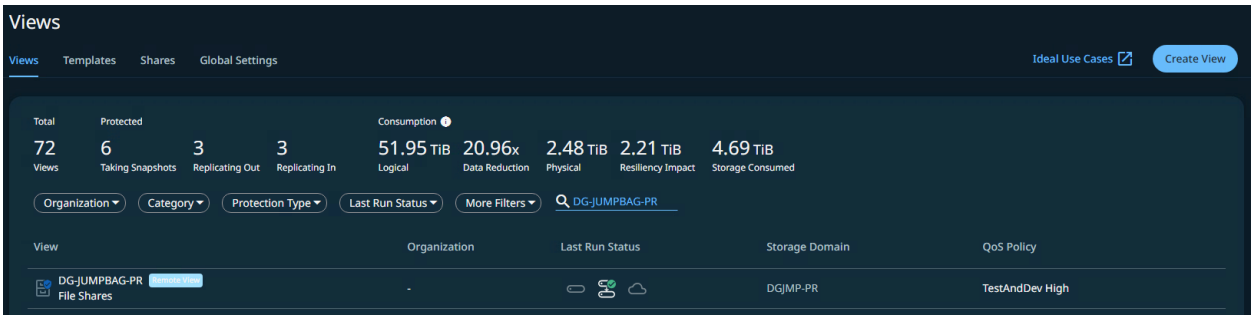
```
[root@orclser /]# mount -t nfs 10.15.1.24:/DG-JUMPBAG-PR /jmpbg
[root@orclser /]# df -h
Filesystem                Size  Used Avail Use% Mounted on
devtmpfs                  7.8G     0  7.8G   0% /dev
tmpfs                     7.8G     0  7.8G   0% /dev/shm
tmpfs                     7.8G   50M  7.8G   1% /run
tmpfs                     7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/mapper/rhel-root      90G   85G  5.5G  94% /
/dev/sda1                1014M  166M  849M  17% /boot
tmpfs                     1.6G   12K  1.6G   1% /run/user/42
tmpfs                     1.6G     0  1.6G   0% /run/user/0
10.15.1.24:/DG-JUMPBAG-PR  61T   17T   44T  28% /jmpbg
```

SmartFiles S3 View

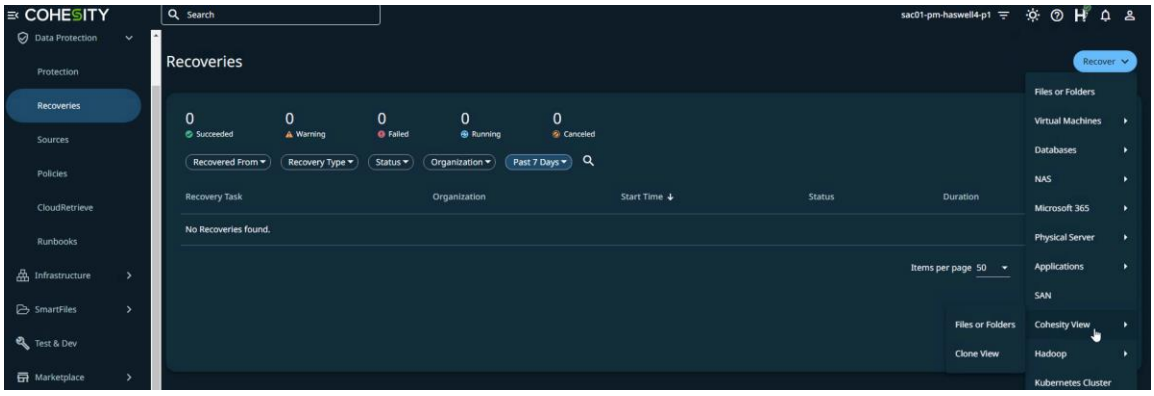
You can directly access S3 View with the access and secret key of the user who created it. In the case of a secondary cluster or remote cluster, you can create the same user on the secondary cluster and access the data.

Isolated Replica Cluster

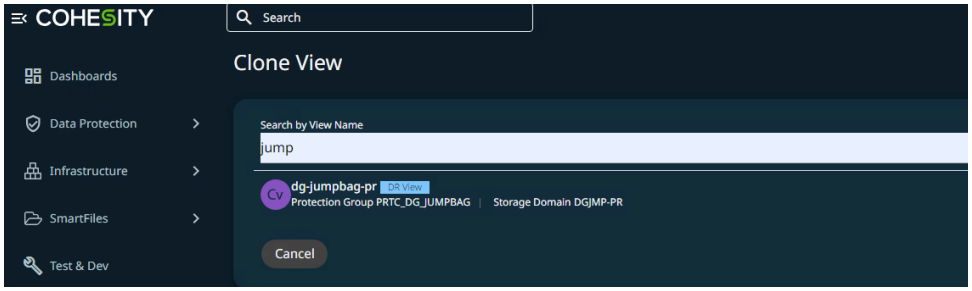
In the Cohesity isolated replica cluster, the SmartFiles view is listed as a Remote View. To access it, follow the steps below.



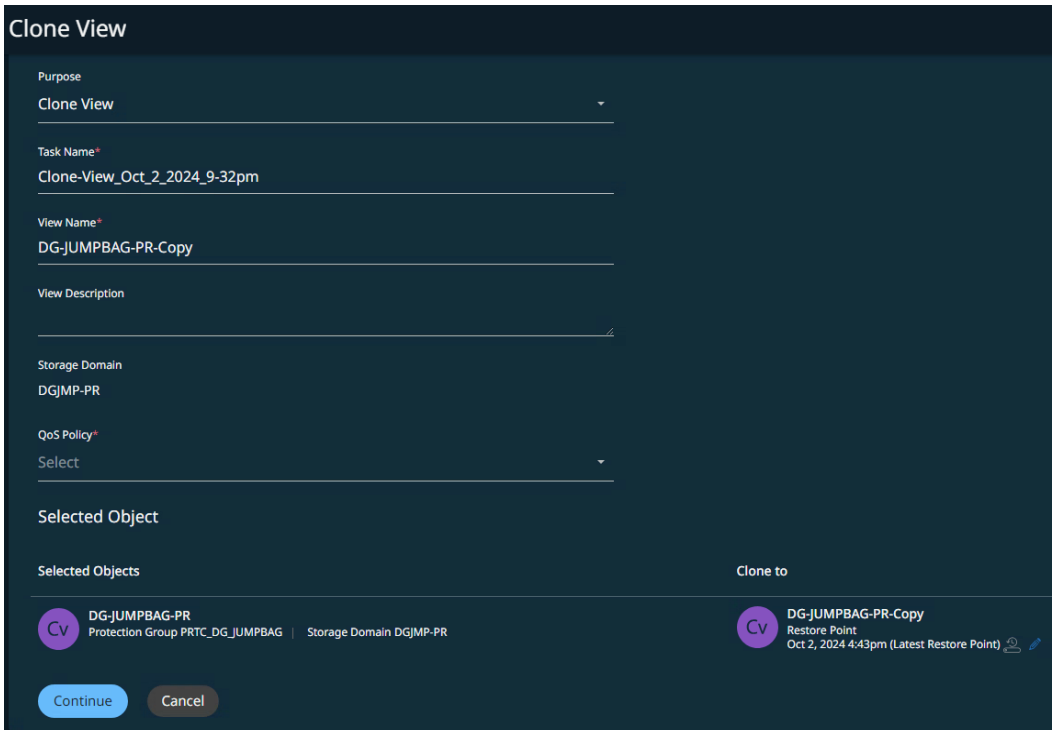
1. Configure the clean room isolated VLAN on the replica cluster as mentioned in sections Create Isolated VLAN on Cohesity Cluster and Create VIPs for the Isolated VLAN.
2. You can recover SmartFiles View from the replica cluster. Navigate to **Data Protection > Recoveries > Recover > Cohesity View > Clone View.**



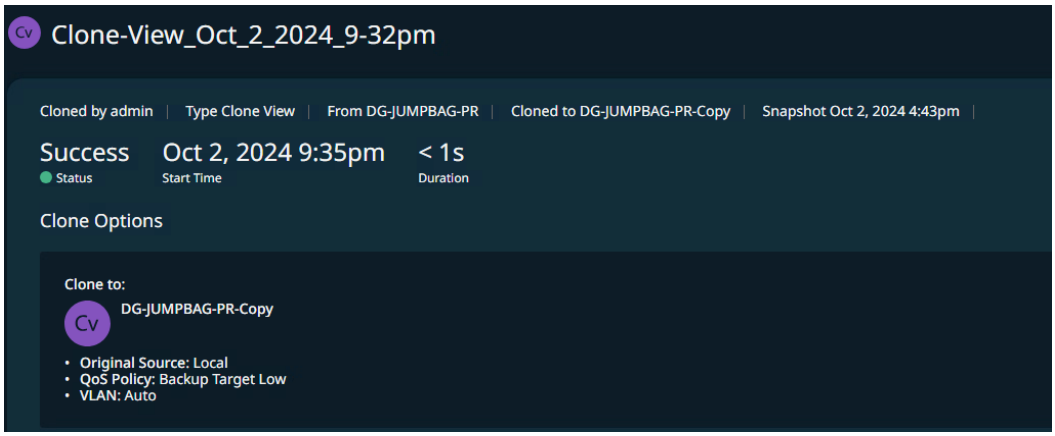
3. Search your view, and it will list it as the “DR View.”



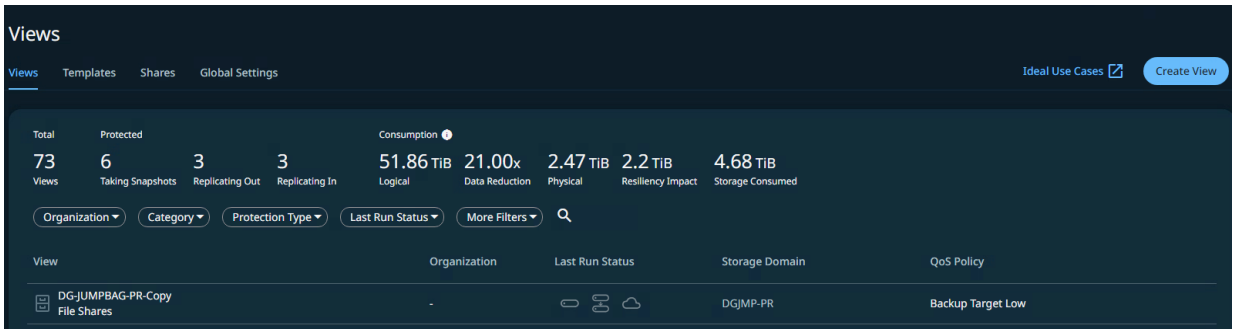
4. Select your view and enter the information as **Task Name**, **View Name**, and **QoS Policy** on the Secondary cluster. Then, select the Snapshot you want to recover from the edit button in **Selected Objects**. Click **Continue**.



5. Check the status of the task. You can access your view once the status is “Success”.



6. Navigate to **SmartFiles** > **View**. Your cloned View will be listed here, and the Remote View tag has been removed.



7. You can edit the View and change its access and permissions with the New authentication service in clean room.

   In case your AD/LDAP or authentication services are impacted and do not serve authentication, Cohesity will allow you to access the data with local authentication. Follow the section Primary Cluster to access the Views in the isolated replica cluster.

Cohesity allows you to recover the file or folders to the View. You can follow this if you don't want to recover/clone the View and only want access to the specific files.

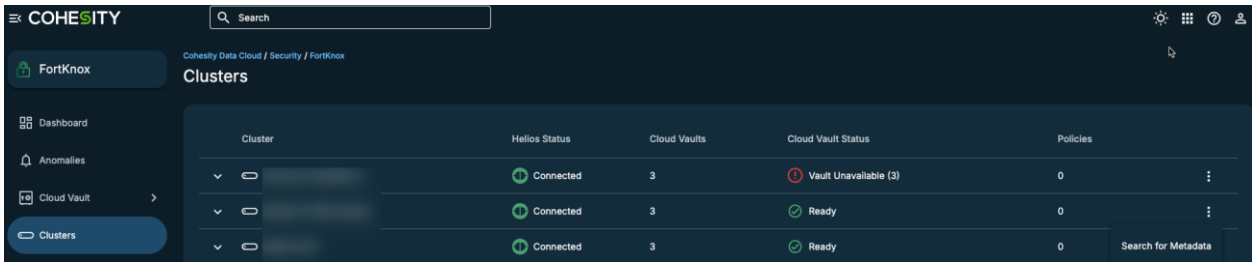
FortKnox

Cohesity FortKnox is a SaaS application that enables you to vault data from the Cohesity cluster to the cloud, recover it from the cloud, and return it to the original or a new destination. It safeguards your data against ransomware attacks, natural disasters or outages, and unauthorized access. In the event of a disaster, if you lose the connection to both primary and replica clusters, you can retrieve your jump bag from FortKnox. The outline of the procedure for the recovery is as follows:

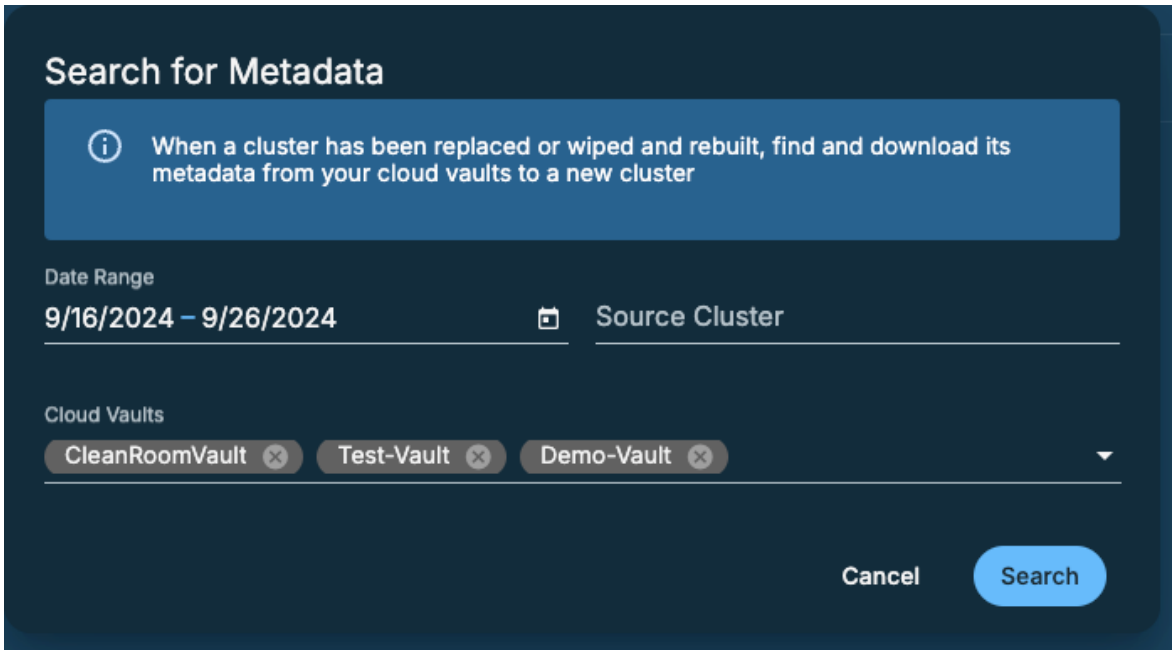
a. A Standby Cohesity Cluster with the Helios Connection is required to retrieve the data from the FortKnox.
b. Retrieve the metadata from FortKnox for the primary cluster, which is no longer operational to the standby Cohesity cluster.
c. Perform the recovery from the Cohesity cluster.

Follow the steps below:

1. Login to Helios and click **Security** > **FortKnox**.
2. You have to retrieve the metadata of the primary cluster to the standby cluster. Navigate to **Clusters > Search for Metadata** on the standby cluster.

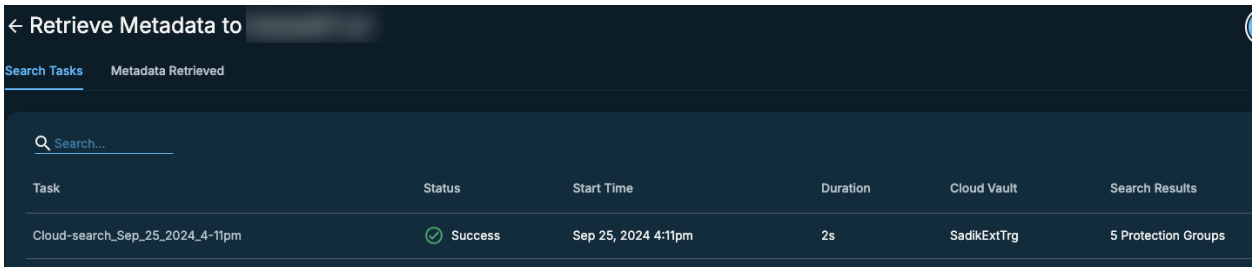


3. Enter the date range and source cluster for which you want to retrieve the metadata and cloud vaults. Click **Search**.

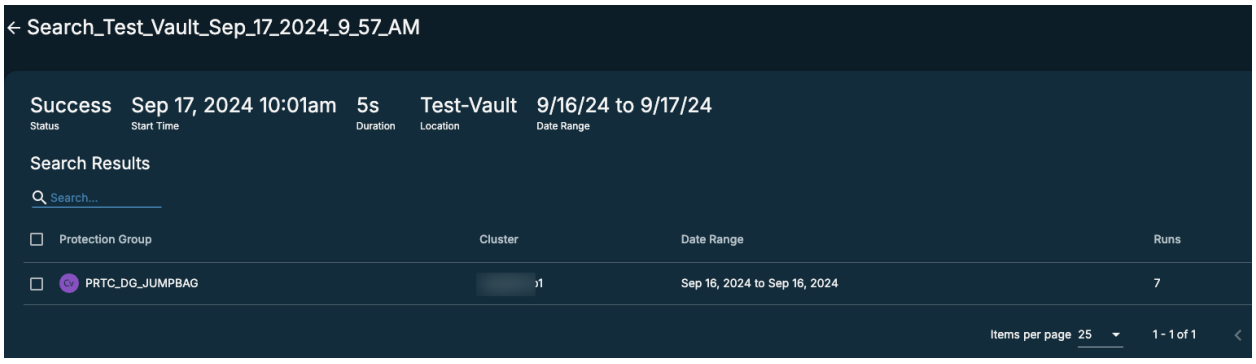


The request will be submitted for quorum approval in case of quorum configuration. Once approved, the metadata search will start.

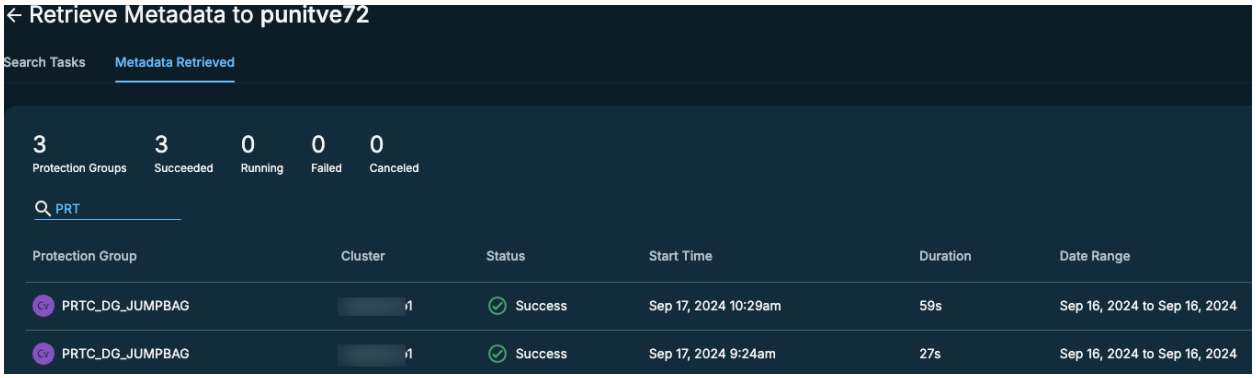
4. Once the search task is complete and the status is “Success,” you can click on it; it will reflect the protection group.



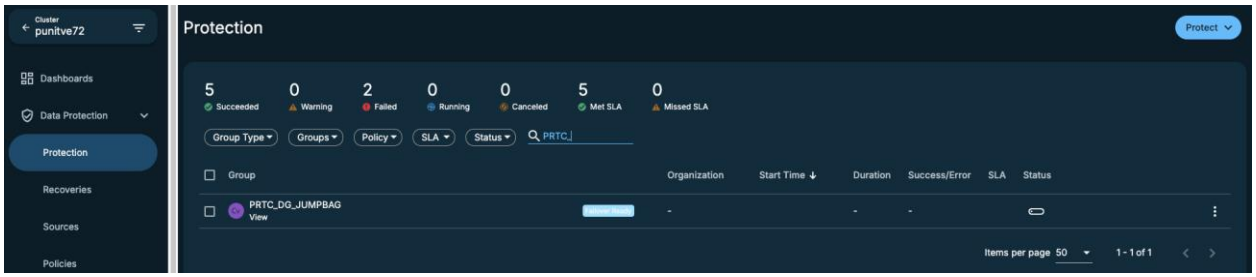
5. Select the protection group inside the search task and click “Download Metadata”. This step will download the metadata to the standby cluster.



6. In the “Metadata Retrieved” section, Monitor the download metadata task. Once the status changes to success, you can perform the Clone View Recovery from the Standby cluster.



7. You can navigate to the Protection tab on the cluster, and the retrieved Protection group will be reflected there.



8. Once the Protection group appears, you can treat the cluster as a secondary cluster or replicated copy. To access the data, follow the Isolated Replica Cluster section.

Configuring Routers and Firewalls

Configuring routers and firewalls in an isolated environment helps control network traffic, secure communications, and prevent unauthorized access, protecting the integrity of the clean room process.

Adhering to best practices is crucial for ensuring security and operational efficiency. Below are some recommendations:

- **Access Rules**: Enforce strict access controls to limit network access to authorized users and devices.
- **Segment Network Traffic**: Utilize VLANs or subnetting to segregate critical systems from non-essential ones, reducing the risk of lateral movement by malicious actors. Refer to Network Isolation for more information.
- **Least Privilege:** Permit only essential communication between systems to limit the attack surface.
- **Strong Authentication:** Enforce multifactor authentication (MFA) for accessing network devices.
- **Logging and Monitoring**: Enable logging and real-time monitoring features to track network activity, detect anomalies, and record access attempts.

Installing the vSphere and ESXi on Physical Server

Installing vSphere and ESXi on a physical server in an isolated environment is crucial in cyber recovery efforts. By utilizing the ISOs and installable from the Digital Jump Bag™, the response team can install the virtual infrastructure needed to create and manage virtual machines, allowing them to run dial-tone applications. Additionally, it provides a secure platform for hosting workloads that are being investigated or restored, ensuring these activities can proceed without risk of further compromise.

NOTE: This guide focuses on setting up VMware-centric hypervisors due to their widespread usage; however, staging with other hypervisors is also possible.

Cohesity can lower the cost and effort of setting up vSphere and ESXi by serving as the datastore for running essential dial-tone applications. Users can utilize Cohesity SmartFiles, which can be mounted as a datastore.

Dial Tone Applications

During a cyber incident, essential business functions such as phone systems, IAMs, emails, and DNS may be compromised. Dial-tone applications are, therefore, crucial for quickly restoring these critical functions, enabling organizations to maintain minimal viable response capabilities while full cyber recovery efforts are in progress.

Response teams can swiftly access the necessary installable and set up dial-tone applications in an isolated environment by using a Digital Jump Bag™, a pre-prepared collection of tools, scripts, and data. Customers can create a separate protection group to identify the dial tone application.

To ensure efficiency and save time, IT teams should deploy dial tone applications from secure, verified sources in an isolated environment during preparation or drills. As a best practice, protect these applications with Cohesity DataProtect and vault them to FortKnox as golden copies. In the event of a cyber incident, response teams can quickly restore the golden copies to the isolated environment. Furthermore, Cohesity allows data to be easily mounted directly from the platform to run dial tone applications, significantly reducing the required storage space and speeding up the recovery process.

For more information on what components to include in a jump bag, refer to the "What's in My Ransomware Jump Bag" blog.

MVRC Checklist

The following checklist guides users through the necessary steps to ensure a successful implementation of the Minimum Viable Response Capability.

Table 6: MVRC Checklist

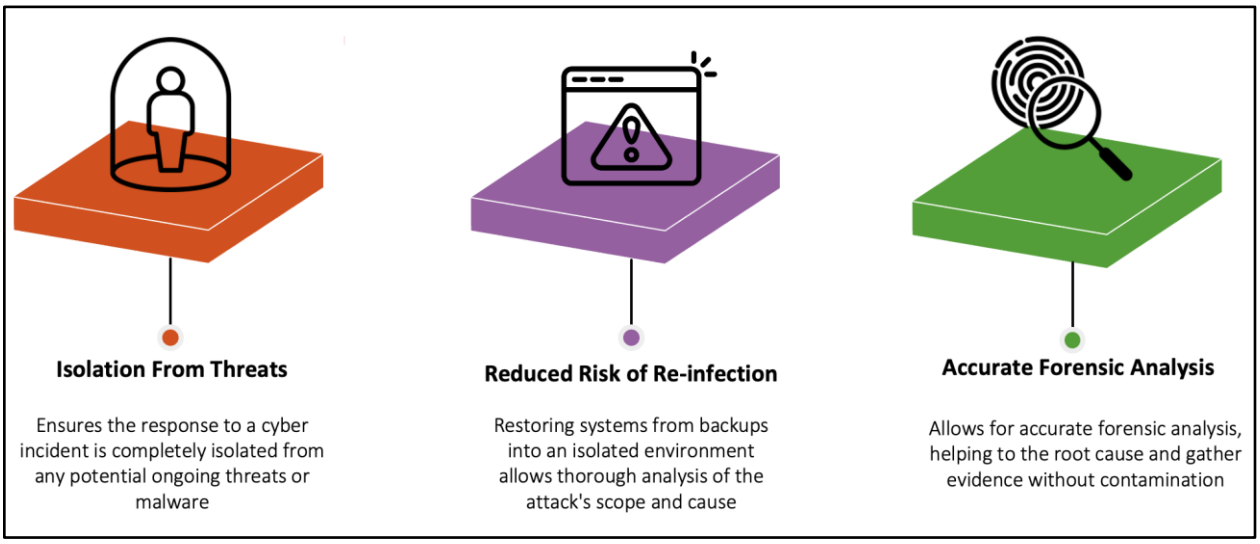
Components	Purpose
Establishing an Isolated Network	Enables teams to investigate, remediate, and restore systems without exposure to ongoing threats, ensuring a secure recovery process.
Connecting Cohesity Cluster to Isolated Network	Secure communication facilitates data transfer from Cohesity DataPlatform to the isolated environment.
Jump Bag Retrieval into Isolated Environment	Ensure all necessary recovery tools, scripts, and documents are accessible within the isolated environment.
Configuring Routers and Firewalls	Set up network controls to ensure secure communication and prevent unauthorized access.
Installing vSphere and ESXi	Deploy virtualization infrastructure to host dial tone applications and investigation workloads within the isolated environment.
Configuring Dial Tone Applications	Ensures critical applications remain operational throughout the cyber recovery process to sustain essential business functions.

Investigate: Clean Room Analysis - Determining Scope and Root Cause

Clean Room plays a critical role in cyber response by providing a secure, isolated environment to respond to cyber incidents. By isolating the response process from any potential ongoing threats or malware, clean room ensures that response efforts are not compromised, reducing the risk of further damage.

Additionally, clean room minimizes the risk of re-infection by restoring systems from backups into a controlled, isolated space. This setup enables thorough analysis of the attack's scope and cause while allowing for accurate forensic investigation to identify the root cause and collect evidence without risk of contamination.

Figure 4: Forensic Analysis



In a cyber recovery scenario, The Isolated environment created in the MVRC becomes the clean room for investigation and root cause analysis. At the end of the investigation process, the infected files, logs, and documents are collected as forensic evidence, and an incident report is provided, which is the outcome of the clean room process.

The investigation phase involves several processes and steps, including

1. Create Forensic Investigation View
2. Setting up a Clean Room Environment
3. Restore Files/Snapshot for Forensic Investigation
4. Forensic Investigation
5. Incidence Report

Create Forensic Investigation View

Forensic evidence collection supplies vital information for legal proceedings and regulatory compliance. It helps attribute responsibility and guides the development of strategies to enhance defenses against future threats.

Cohesity recommends creating a SmartFile view for forensic evidence collection. Creating a forensic evidence view involves similar steps to setting up a Digital Jump BagTM View. Once the forensic view is created, it can be mounted onto a forensic workstation in the clean room. The steps to mount a view into an isolated environment are outlined here. Users can choose how long to retain backed-up data on Cohesity, depending on the nature of the attack.

Cohesity recommends following the 3-2-1+ strategy for data management to protect the Forensic Investigation View after evidence collection.

Setting up a Clean Room Environment

This section will outline the steps required to set up a clean room environment. The ESXi hosts and vCenter environment are configured for clean room analysis. To set up the clean room environment, refer to the steps mentioned in Installing the vSphere and ESXi on Physical Server. The snapshots from Cohesity production or replica clusters are recovered to the clean room environment for threat analysis.

Register Clean Room vCenter or Equivalent to the Cohesity Cluster

The first step in clean room configuration is registering the clean room (VMWare vCenter source) on the Production or Replication Cohesity cluster. Assuming the isolated VLAN has been configured on the Cohesity cluster (refer to the Network Isolation section for steps to configure the isolated VLAN).

Follow the Register Source (vCenter) steps in the Appendix section to register the vCenter source.

Restore Files/Snapshots for Forensic Investigation

In the investigation stage, the snapshots available on the Cohesity cluster (Production, Replication, or FortKnox) are leveraged for forensic examination. The snapshots provide the security engineers with the events' timeline and help identify the latest clean snapshot.

To perform the forensic analysis, we require the following components:

Table 7: Components Required for Forensic Analysis

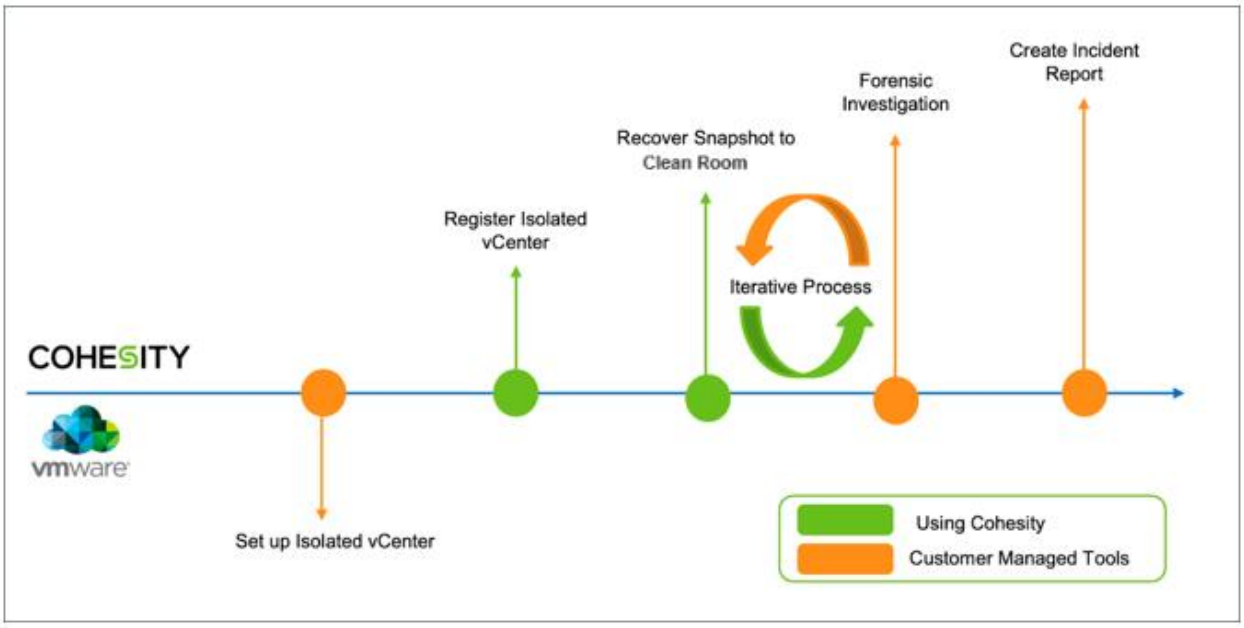
Component	Definition and Use Case
Cohesity cluster	Production or Replication Cohesity clusters can serve as a source of snapshots for investigation.
SmartFiles View	A Data Locked Evidence Collection view. This view is mounted on the forensic workstation.

Component	Definition and Use Case
	For more information on SmartFiles View. Refer to the Digital Jump Bag™ section.
Forensic workstation	A physical server running either Windows or Linux. The forensic workstation connects to the clean room and Cohesity cluster. It has access to the Jumpbox view for forensic evidence collection.
Security Tools	Enable external security tool access to clean room workloads. Analyze the workloads for anomalies and perform the RCA.

Workflow

The workflow in the diagram below is followed during the clean room investigation.

Figure 5: Clean Room Investigation Workflow



Cohesity Recovery Methods

This step involves moving the historical snapshots of the workloads to the clean room for forensic analysis. In this workflow, the VMs will be recovered to a "**New Location**," i.e., the clean room vSphere cluster, as the production vSphere cluster may not be trusted.

The workflow applies to recovering workloads from the Customer Managed Cohesity production cluster, replication cluster, or FortKnox.

Recovery Methods

Depending on your security team's decision, you may need to recover files, folders, or VMs (snapshots). Cohesity DataProtect offers various recovery methods based on the security team's decisions. Choose the right recovery method below:

Table 8: Cohesity Recovery Methods

Recovery Method	Definition	Use case
File/Folder Recovery	Cohesity allows you to recover files and folders from a snapshot created earlier by a Protection Group. Files and folders can be recovered to their original location or a newly specified location, within the original source or a different one.	1. Only some identified files/folders need to be recovered for analysis. 2. Target VM is available at the clean room cluster to recover the files/folders. The VM could contain security tools to analyze data. 3. Cohesity agent or VMware Tools should be installed on the target VM. (Can be deployed during the recovery process) 4. Identified files can be downloaded locally to the forensic workstation for investigation.
VM Recovery	Cohesity provides the ability to recover Protected Objects (such as VMs) from a snapshot created earlier by a Protection Group. You can recover VMs from a Cohesity cluster to their original or new location.	Recover the complete VM to the clean room cluster for analysis.
Disk Recovery	Cohesity allows you to recover VMware VM virtual disks to a point in time from a Snapshot created by a Protection Group. You can	1. Only a particular vDisk is identified for analysis, not the complete VM.

Recovery Method	Definition	Use case
	recover a virtual disk to its original VM or a different VM in the same or a different vCenter.	2. Target VM is available to restore the vDisk as a new disk and analyze it for malicious content. 3. Datastore is available at the clean room cluster for vDisk recovery.
Instant Volume Mount	Instant volume mounting is supported for virtual and physical environments. This feature makes the selected backup volumes available at the target location, where you can complete the desired operations.	1. Instant access to the volumes. 2. No datastore is required at the clean room cluster. 3. A Cohesity agent is not required at the target VM. 4. Access to files directly from the Cohesity cluster. 5. On-demand teardown.

For virtual machines, Cohesity allows you to instantly recover VMs or perform Copy Recovery, depending on the requirements and resource availability.

Recovery Method	Definition
Instant Recovery	After recovery, the VMs will be instantly available in the target location, and the data will be moved to the target storage later. During Instant Recovery, the VM can be used in production when data is copied from the Cohesity cluster. With Instant Recovery, the VMs will be instantly available for forensic analysis on the clean room cluster.
Copy Recovery	The VMs will be available in the target location only after all the data is copied to the target storage **(Clean Room or Staging cluster)** from the source location (Cohesity cluster). Once the restore is complete, the VM will be available to use, and its performance will be normal. Cohesity recommends Copy Recovery for powered-off VMs for better performance.

Recover from Customer-Managed Cohesity Cluster

In this recovery method, the data is recovered from the Customer Managed Cohesity cluster, which can be the production or replication cluster.

File/Folder Recovery

Cohesity allows you to recover files and folders from a snapshot created by a Protection Group and recover them to the clean room cluster for forensic analysis. Follow the File/Folder Recovery steps in the Appendix section to recover files and folders.

Alternatively, Cohesity allows you to download the files and folders from the selected snapshot of the Protection Group locally on your system. This workflow can help in fast analysis where the suspected malicious files are downloaded on the local jump host. The security persona can then use the security tools to investigate the downloaded files for malicious content. Follow the Download Files/Folders steps in the Appendix section to download files and folders to your local system.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

VM Recovery

Cohesity provides the ability to recover Protected Objects (such as VMs) from a snapshot created earlier by a Protection Group. You can recover VMs from a Cohesity cluster to the clean room cluster for forensic analysis. Follow the VM Recovery steps in the Appendix section to recover the VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Virtual Disk Recovery

Cohesity allows you to recover VMware VM virtual disks to a point in time from a Snapshot created by a Protection Group. You can recover a virtual disk to the clean room cluster for forensic analysis. Follow the Virtual Disk Recovery steps in the Appendix section to recover the VM virtual disks.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Instant Volume Mount

Instant volume mounting is supported for virtual and physical environments. This feature makes the selected backup volumes available at the target location, where you can complete the desired operations. The volume is available instantly to perform forensic analysis and tear down when needed.

Follow the Instant Volume Mount steps in the Appendix section to mount volumes on the target VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Recover from FortKnox

Alternatively, you can recover snapshots from FortKnox to the clean room cluster. Cohesity FortKnox allows you to recover your cluster data from a cloud vault. You can perform the below operation on the workloads from a cloud vault.

1. Recover Databases
2. Recover NAS
3. Recover Physical Servers
4. Recover VMware Virtual Machines
5. Clone Cohesity View

In a disaster, if you lose the connection to both primary and secondary clusters, you can retrieve your data (files/folders, virtual disks, or VM) from FortKnox. The procedure outline for the recovery is as follows:

a. A standby Cohesity cluster with a Helios connection is required to retrieve the data from Fort Knox.
b. Retrieve the metadata from FortKnox for the primary cluster, which is no longer operational, and the standby Cohesity cluster. Refer to the Download Metadata to the Standby Cohesity Cluster for steps to perform this operation.
c. Perform the recovery from the Cohesity Cluster.

The Protection Groups are available on the standby cluster, where you can choose one of the recovery methods below to get the data to the clean room.

1. File/Folder Recovery.
2. VMs.
3. Virtual Disks Recovery.
4. Instant Volume Mount for the VMs.

File/Folder Recovery

Cohesity allows you to recover files and folders from a snapshot in the cloud vault. In this workflow, the files/folders are recovered to a New Location, the clean room cluster.

Follow the File/Folder Recovery steps in the Appendix section to recover files and folders.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Alternatively, Cohesity allows you to download the files and folders from the selected snapshot of the Protection Group locally on your system. This workflow can help in fast analysis where the suspected malicious files are downloaded on the local jump host. The security persona can then use the security tools to investigate the downloaded files for malicious content.

Follow the Download Files/Folders steps in the Appendix section to download files and folders to your local system.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

VM Recovery

Cohesity allows you to recover protected objects from the cloud vault, such as VMware VMs. You can recover VMs to the clean room cluster using the cloud vault i.e., FortKnox.

Follow the VM Recovery steps in the Appendix section to recover the VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Virtual Disk Recovery

You can recover VMware VM virtual disks to a point in time from a snapshot created by a Protection Group. You can recover a virtual disk to its original VM or a different VM in the same or a different vCenter. In this scenario, we will recover the virtual disk to a new location, VM in the clean room cluster.

Follow the Virtual Disk Recovery steps in the Appendix section to recover the VM virtual disks.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Instant Volume Mount

Instant volume mount allows the selected backup volumes to be available at the target location, where you can complete the desired operations. In this scenario, the target volume can be mounted on a VM in the clean room cluster for analysis.

Follow the Instant Volume Mount steps in the Appendix section to mount volumes on the target VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Forensic Investigation

Clean Room forensic investigation is essential for an effective cyber response, offering a controlled, isolated environment to analyze attacks without risk of contamination. It preserves evidence integrity and identifies the root cause and scope of the attack.

Based on intelligence from external detection sources and/or Cohesity's native detection capabilities, the necessary snapshots for forensic investigation are made available within the clean room. This investigation is an iterative process that involves examining snapshots from various points in time and may require multiple steps, including but not limited to the following actions.

1. Leveraging DataHawk
2. Involve Incident Response Teams
3. Compare AD Changes
4. Collect Forensic Evidence

DataHawk for Forensic Investigation

Cohesity DataHawk offers comprehensive security features, including threat hunting for Indicator of Compromise (IOC) detection and data classification for thorough impact analysis.

Cohesity Threat Detection supports forensic investigation by allowing customers to trigger threat scans on snapshots designated for forensic analysis (i.e., those that will be mounted or moved to a clean room). The results of these scans provide investigators with crucial intelligence to aid in their efforts.

Cohesity Threat Hunting enhances threat detection through built-in feeds that scan for over 117,000 IOCs. It also enables targeted threat hunting by allowing customers to upload custom YARA rules. Additionally, Cohesity's integration with CrowdStrike Falcon Adversary Intelligence provides advanced scanning capabilities, helping users quickly identify new and evolving threats.

Cohesity's DataHawk Data Classification provides a comprehensive, enterprise-grade classification for backup data, identifying multiple data patterns out-of-the-box to meet various compliance and regional mandates. Identifying critical PII in affected workloads facilitates impact assessment and helps uncover potential data compromises through exfiltration.

Adopting best practices by scheduling weekly threat scans and monthly data classifications ensures investigators have readily available information, significantly reducing time spent during investigations.

NOTE: Threat Detection and Data Classification scans are supported only on snapshots stored on a Cohesity cluster or a replicated copy of the snapshots. Currently, scans are not possible for archival copies retrieved from FortKnox or other archival targets.

Refer to the Get Started with Cohesity DataHawk documentation for instructions on configuring Data Classification and Threat Protection scans.

Incident Response Teams and External Security Tools

Incident response teams are critical in identifying, managing, and mitigating security incidents. Many Security organizations and federal agencies recommend involving incident response teams in managing cyber incident scenarios.

Incident response teams follow a multi-step process to identify, manage, and resolve security threats, thoroughly documenting each stage from initial detection to final recovery. This documentation includes a comprehensive incident report detailing the event's nature, causes, impact, response actions, and lessons learned.

Additionally, the team performs a post-incident review to assess the effectiveness of the response, pinpoint any gaps or weaknesses in existing processes, and suggest improvements to enhance future defenses.

NOTE: Ensure that firewalls are set to enable communication between the Clean Room and the external security tools utilized by Incident Response teams.

Compare AD Changes

In a cyber recovery scenario, comparing Active Directory changes is crucial to identifying any unauthorized modifications, detecting potential security breaches, and ensuring the integrity of user accounts, permissions, and configurations. This comparison helps verify that no malicious changes have persisted and that the environment is restored to a secure, trusted state.

Cohesity DataProtect helps protect your Active Directory (AD) and offers a user-friendly interface for comparing different AD snapshots. This enables investigators to detect any unauthorized modifications that may have persisted quickly.

Forensic Evidence Collection

In a cyber recovery scenario, forensic evidence is gathered to support in-depth forensic analysis, including the simulation of the attack in a controlled sandbox environment. This evidence is critical for identifying the root cause, assessing the impact, and supporting legal or regulatory actions. The following key information is typically gathered as forensic evidence:

- System and application logs
- Network traffic data
- Malicious files and executables
- User activity records and access logs
- Configuration changes and system modifications
- Memory dumps and disk images
- Evidence of unauthorized access or privilege escalation
- Backup and snapshot data for comparison

This comprehensive collection enables a detailed forensic investigation, which helps ensure accurate analysis and effective remediation.

Protecting and data-locking ensures it remains tamper-proof once forensic evidence is collected into the view. As a best practice, archiving the forensic evidence view in FortKnox further enhances its security. This approach helps in establishing a transparent chain of custody, which is required for the evidence to be admissible in court.

The steps to protect a Forensic Investigation View are similar to those for securing a Digital Jump BagTM View.

Incident Report

An Incident Report is a vital document that is the outcome of a Clean Room Investigation. It offers a detailed account of the event and remediation actions to be taken. This report is crucial for thoroughly understanding the incident, directing remediation efforts, ensuring regulatory compliance, and enhancing security measures to prevent future occurrences.

An Incident Report following a forensic investigation typically includes details such as the scope and nature of the incident, timeline of events, root cause analysis, identified vulnerabilities, impact assessment, evidence collected, remediation actions, and recommendations for future prevention and becomes a baseline for Mitigation efforts.

Mitigate: Staging Room for Remediation

In the mitigation phase, workloads are prepared for remediation within an isolated staging room. In this controlled environment, data and systems undergo comprehensive remediation and validation, addressing Indicators of Compromise (IOCs), applying patches, managing vulnerabilities, conducting data integrity checks, and performing integration testing. This helps ensure that all assets are free from threats or corruption. By using a staging room, organizations can confidently verify the security and integrity of their systems, reducing the risk of reinfection or disruption before safely returning them to the production environment.

The complexity and importance of this phase demands a well-orchestrated, multi-step process that involves collaboration across various teams. In this section, we will cover the following key topics:

1. Using a Jump Bag in the Staging Room
2. Setting Up Your Staging Environment
3. Recover vs. Rebuild
4. Recover System & Data
5. Remediation Steps
6. Protect the Remediated Systems

Jump Bag: Retrieval Strategies for Staging Environments

In situations where you need to access the Jump Bag for ISO files or installation scripts, follow the same procedure outlined in Digital Jump Bag™: Retrieval Strategies for Isolated Environment.

Setting Up a Staging Environment

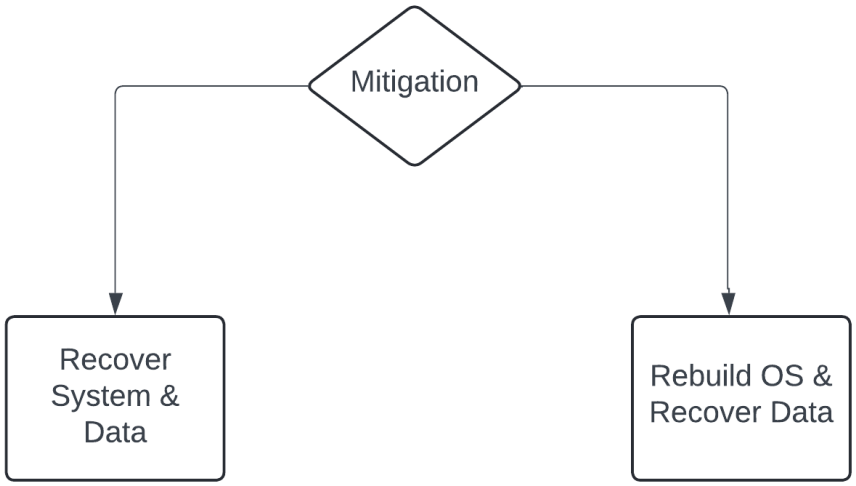
This section will outline the steps required to set up a staging environment. The ESXi hosts and vCenter environment are configured to perform remediation in the staging rooms. To set up the staging room environment, refer to the steps mentioned in Installing the vSphere and ESXi on Physical Server. This configuration provides snapshots from Cohesity production or replica clusters for threat analysis.

NOTE: We have focused on setting up VMware-centric hypervisors in this guide due to the widespread usage; however, staging with other hypervisors is also possible.

Design Decision—Recover & Clean Vs Rebuild from Golden Image

During the cyber recovery process, organizations often encounter critical decisions, such as whether to restore systems from backups or rebuild them entirely. This choice is particularly significant as it involves multiple teams and must consider various factors, including the severity of the attack, business service level agreements (SLAs), and the complexity of the environment. Consequently, a meticulous decision-making process is essential to ensure effective recovery. The MITRE ATT&CK framework serves as a valuable tool in guiding these decisions, providing a structured approach to assess and address the intricacies of each situation.

Figure 6: Design Decisions—Recover Vs Rebuild



Using the MITRE ATT&CK framework to map out and understand the tactics and techniques employed in an attack provides valuable insights into the severity and impact of the compromise. This detailed understanding is crucial in deciding whether to **recover** the existing system or to **rebuild** it entirely. Factors such as the extent of the compromise, available resources, and the potential for residual threats should guide your decision to ensure system integrity and organizational security.

Recover & Clean

Once the snapshot has been identified as safe to restore to staging, it can be recovered from the production, replication cluster, or FortKnox to the staging room, where necessary action is taken to mitigate all the security gaps and create a golden copy for clean recovery.

The remediation steps can include (but not limited to):

1. IOC remediation
2. Patching
3. Vulnerability fix
4. Security Hardening
5. Integration Testing

Refer to the Remediation Steps section for more information.

Recover from Customer-Managed Cohesity Cluster

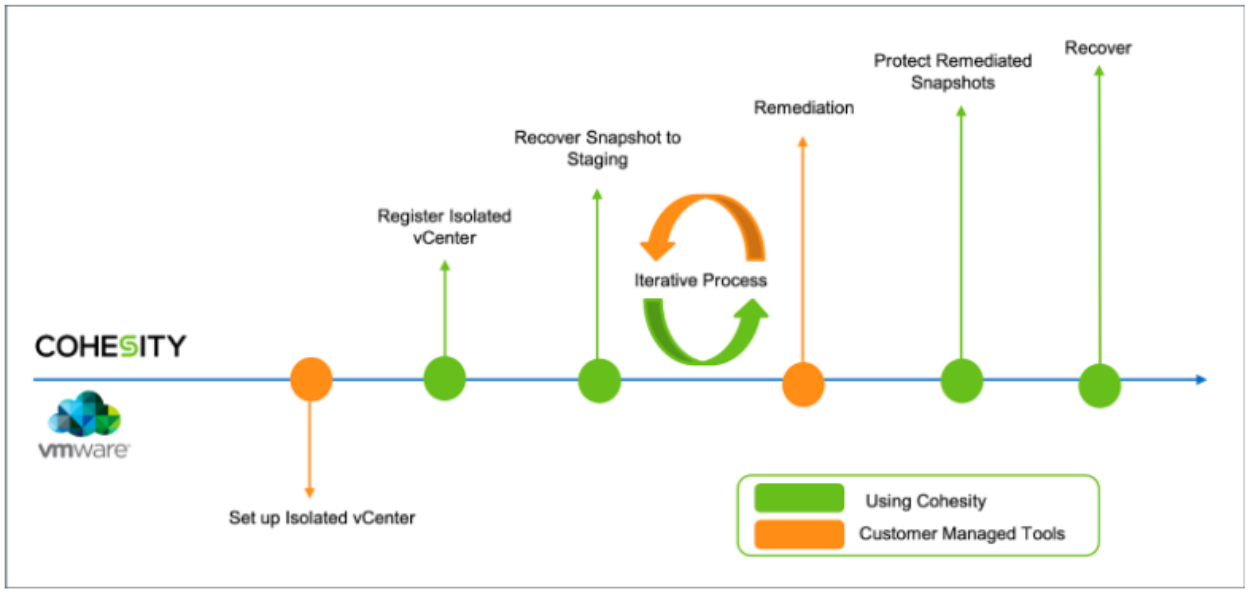
In this recovery method, the data is recovered from the Customer Managed On-Premise Cohesity cluster, which can be the production or replication cluster.

Follow the steps below to recover snapshots from the Production/Replication cluster.

Workflow

The workflow in the diagram below is followed during mitigation.

Figure 7: Mitigation Workflow



Register Staging Cluster

The first step in the remediation stage is registering the staging (vCenter) cluster on the Production or Replication cluster. Assuming the isolated VLAN has been configured on the Cohesity cluster (refer to the Network Isolation section for steps to configure the isolated VLAN).

Follow the Register Source (vCenter) steps in the Appendix section to register the vCenter source.

Recover Snapshots to Staging Room

This step involves moving the last clean snapshot identified in the investigation stage to the staging cluster for mitigation. In this workflow, the VMs will be recovered to a "**New Location**," i.e., the staging cluster, to mitigate and create a golden copy.

The workflow below applies to recovering workloads from the Customer Managed On-Premise Production or Replication cluster to the clean room cluster.

Recovery Methods

For various methods of recovering VMs, files, folders, virtual disks, or mounting disks to the staging cluster, refer to the Methods of Recovery section.

File/Folder Recovery

Cohesity allows you to recover files and folders from a snapshot created by a Protection Group and recover them to the staging cluster for remediation. Follow the File/Folder Recovery steps in the Appendix section to recover files and folders.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

VM Recovery

Cohesity provides the ability to recover Protected Objects (such as VMs) from a snapshot created earlier by a Protection Group. You can recover VMs from a Cohesity cluster to the staging vCenter for remediation. Follow the VM Recovery steps in the Appendix section to recover the VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Virtual Disk Recovery

Cohesity allows you to recover VMware VM virtual disks to a point in time from a Snapshot created by a Protection Group. You can recover a virtual disk to the staging vCenter for remediation. Follow the Virtual Disk Recovery steps in the Appendix section to recover the VM virtual disks.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Instant Volume Mount

Instant volume mounting is supported for virtual and physical environments. This feature makes the selected backup volumes available at the target location, where you can complete the desired operations. The volume is available instantly to perform remediation and tear down when needed. Follow the Instant Volume Mount steps in the Appendix section to mount volumes on the target VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Recover from FortKnox

Alternatively, you can recover snapshots from FortKnox to the clean room cluster. Cohesity FortKnox allows you to recover your cluster data from a cloud vault. You can perform the below operation on the workloads from a cloud vault.

1. Recover Databases
2. Recover NAS
3. Recover Physical Servers
4. Recover VMware Virtual Machines
5. Clone Cohesity View

In a disaster, if you lose the connection to both primary and secondary clusters, you can retrieve your data (files/folders, virtual disks, or VM) from FortKnox. The outline procedure for the recovery is as follows:

1. A standby Cohesity cluster with a Helios connection is required to retrieve the data from Fort Knox.
2. Retrieve the metadata from FortKnox for the primary cluster, which is no longer operational, and the standby Cohesity cluster. Refer to the Download Metadata to the Standby Cohesity Cluster for steps to perform this operation.
3. Perform the recovery from the Cohesity Cluster.

The Protection Groups are available on the standby cluster, where you can choose one of the recovery methods below to get the data to the clean room.

1. Files and folders
2. VMs
3. Virtual Disks
4. Instant volume mount for the VMs

File/Folder Recovery

Cohesity allows you to recover files and folders from a snapshot in the cloud vault. In this workflow, the files/folders are recovered to a New Location, the staging cluster.

Follow the File/Folder Recovery steps in the Appendix section to recover files and folders.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

VM Recovery

Cohesity allows you to recover protected objects, such as VMware VMs, from the cloud vault. You can recover VMs to the clean room cluster using the cloud vault i.e. FortKnox. Follow the VM Recovery steps in the Appendix section to recover the VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Virtual Disk Recovery

You can recover VMware VM virtual disks to a point in time from a snapshot created by a Protection Group. You can recover a virtual disk to its original VM or a different VM in the same or a different vCenter. In this scenario, we will recover the virtual disk to a new location, VM in the staging cluster. Follow the Virtual Disk Recovery steps in the Appendix section to recover the VM virtual disks.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Instant Volume Mount

Instant volume mount allows the selected backup volumes to be available at the target location, where you can complete the desired operations. In this scenario, the target volume can be mounted on a VM in the clean room cluster for analysis. Follow the Instant Volume Mount steps in the Appendix section to mount volumes on the target VM.

By default, the latest snapshot is selected for recovery. To recover older snapshots for analysis, follow the steps in Recover Older Snapshots.

Rebuild from Golden Image

In some scenarios, the end user can decide to recover from the golden image. The golden image is a customer-provided ISO with all the vulnerability fixes. The VMs are built from the golden image. The data is recovered from the Cohesity cluster, which could be the production or replication cluster or FortKnox.

The Golden Image can be mounted from the SmartFiles View or a customer-provided repository. Once the system is built from the golden ISO, depending on the requirement, follow the recovery methods below to recover data.

Recovery Methods

When recovering from the Cohesity cluster, you can choose to either recover the virtual disk to the target VM or provide an instant volume mount from the Cohesity cluster. Alternatively, if you need to recover only some files or folders, you can opt for file/folder recovery.

Table 9: Recovery Methods

Recovery Method	Use case
File/Folder Recovery	1. Cohesity agent should be installed on the target VM. (Can be deployed during the recovery phase) 2. Faster recovery. 3. Recover only the selected identified files/folders to the target VM.
Virtual Disk Recovery	1. Recover the identified vDisk to the VM. 2. Faster recovery. 3. The datastore should be available at the target for recovering as a new disk.
Instant Volume Mount	1. Instant access to the volumes. 2. No datastore is required at the clean room cluster. 3. Access to files directly from the Cohesity cluster. 4. On-demand teardown.

Recover from Customer-Managed Cohesity Cluster

In this recovery method, the data is recovered from the Customer Managed On-Premise Cohesity cluster, which can be the production or replication cluster.

File/Folder Recovery

Cohesity allows you to recover files and folders from a snapshot created earlier by a Protection Group. In this workflow, the files/folders are recovered to the VM created from the Golden ISO at a New Location.

The steps for recovering files/folders from the production or replication cluster to the new VM remain the same. Refer to the File/Folder Recovery section for steps to recover files or folders to the staging room.

Virtual Disk Recovery

Cohesity allows you to recover the virtual disks to the New Location, here it is the VM created from the Golden ISO. The virtual disks are recovered as New Disks and onto a new available datastore.

The steps for recovering virtual disks from the production or replication cluster to the new VM remain the same. Refer to the Virtual Disk Recovery section for steps to recover virtual disks to the staging room.

Instant Volume Mount

Cohesity allows you to make data instantly available on the VM via Instant Volume Mount. The VM can access the data on a snapshot on the Cohesity cluster. The end user can continue to access the data on the mounted volume and tear down when required. It eliminates the need for a datastore at the target location. When a datastore is mounted, the user can plan to recover the virtual disk or copy the data from the volume mount and tear down the volume. The process is seamless and instantaneous.

The steps for mounting volumes from the production or replication cluster to the staging room remain the same. Refer to the Instant Volume Mount section for steps to recover mount volumes to the staging room.

Remediation Steps

The Incident Report, shared as the outcome of the Clean Room Activity, offers essential guidance for remediating the affected workloads. This step is critical, as it involves standing up the system from a recommended baseline snapshot and requires various remediation activities involving multiple teams. The remediated snapshot(s) will be the version that will be recovered to production.

This section outlines all potential remediation steps and identifies the teams responsible for each activity. The table below provides a summary of the remediation steps for a quick reference.

Table 10: Remediation Procedures

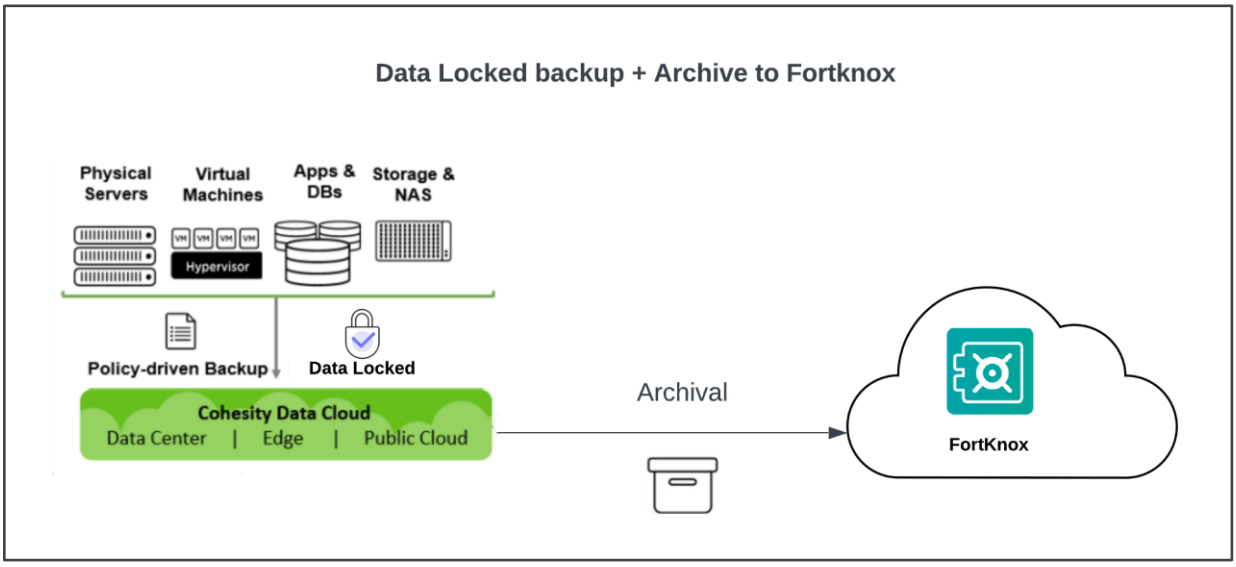
Remediation Step	Purpose	Teams Responsible
IOC Remediation	Identify and remove signs of compromise to restore system security and prevent future attacks.	Security
Patching	Address known issues or update software systems to prevent exploitation by threats.	IT
Vulnerability Fix	Address security weaknesses and loopholes in systems to prevent exploits and attacks, which may include patching the systems.	IT
System Hardening	Enhance a system's security by minimizing its attack surface and applying security controls to guard against threats and unauthorized access.	IT / Security
Integration Testing	Ensures that different components and systems work together seamlessly and identify and resolve any issues before deployment to the production environment. This is the first time all systems are brought up together, assigned IP addresses, and communicate with one another. It is crucial that all systems successfully pass the integration test.	IT / Application Team

Protect Remediated Systems

Once the systems are remediated and successfully pass integration testing, it is crucial to protect them. Securing these remediated systems provides customers with a trusted baseline or snapshot to restore if a system needs to be recovered later or if it becomes compromised again.

Adopting the 3-2-1+ strategy for data management, which involves maintaining a data-locked backup alongside an archive with a longer retention period, is an effective approach to protecting remediated systems. Cohesity FortKnox is a preferred solution in this context, serving as an isolated archive that only connects to the system during data writing or restoration processes. This ensures that in the event customers need to access remediated systems, a secure, reliable, and immutable copy is always available in FortKnox, providing an added layer of protection and peace of mind.

Figure 8: Protect Remedated Systems



Protecting a Virtual Machine is a quick three-step process.

1. **Register the Source**: Verify that the hypervisor is added as a source on the Cohesity Cluster.
2. **Set up Protection**
    a. In the Cohesity UI, use the left navigation panel to select **Data Protection**, then choose **Protection**.
    b. Navigate to the top-right corner, click **Protect**, and then select **Virtual Machines**.
    c. In the pop-up window, add the objects to be protected, assign a name to the protection group, select the appropriate policy, and choose the target storage domain.
    d. Click Protect to complete the step
3. **Validation:** Navigate to **Data Protection** > **Protection** to view the status of your protection groups.

Refer to Add or Edit a Protection Group for Virtual Servers for protection and refer to the section for vaulting the data to FortKnox.

Recover from FortKnox

In this recovery method, the data is recovered from FortKnox.

Similar to using the Customer Managed On-Premise cluster, with FortKnox, you can perform the below recoveries:

1. File/Folder recovery
2. VM recovery
3. Virtual Disk Recovery

Recovery

Restoring systems to production is a crucial element of Cyber Recovery, demanding meticulous planning and execution to ensure systems are returned to their fully-functional state prior to a security incident. This section outlines the essential steps for a controlled and secure recovery, including the final validation procedures and strategic approaches.

The process involves several key stages:

1. Performing last-mile validation to ensure a confident recovery
2. Replication from Staging to Production
3. Initiating the recovery
4. Obtaining quorum approval to prevent unauthorized actions
5. Validating the restored production environment

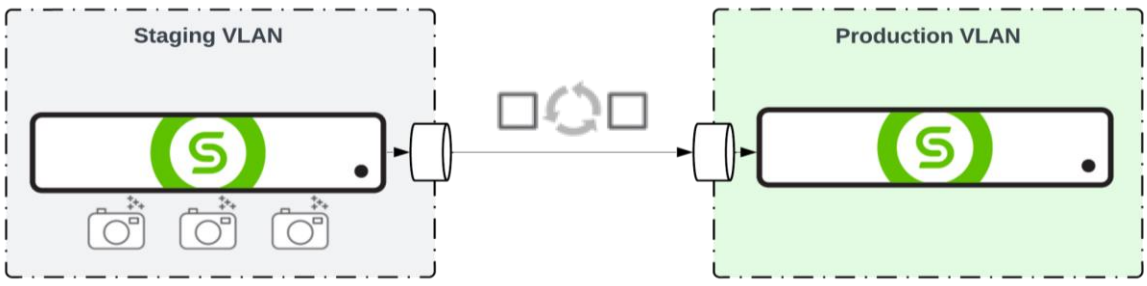
Last Mile Validation

A key advantage in ensuring a secure recovery process is the capability to scan backups for threats before restoring workloads to production. Cohesity enhances this process by integrating Threat Hunting with its DataHawk feature, allowing for the detection of emerging threats. For example, Cohesity's integration with CrowdStrike Falcon Adversary Intelligence enables users to identify emerging threats quickly, with updates refreshed daily. This constant update ensures a thorough final validation, providing users with the confidence needed for a secure and reliable recovery.

Cohesity Data Replication: From Staging to Production

Once final validation is complete, the data is ready for recovery to the production environment. In scenarios where the staging environment has its own Cohesity Cluster, the data must first be replicated from the Cohesity Cluster in the Staging VLAN to the Cohesity Cluster in the Production VLAN. Therefore, snapshots of the remediated systems need to be replicated in the Production Cohesity Cluster before proceeding with recovery.

Figure 9: Cohesity Replication—Recover to Production



For more information on setting up replication between Cohesity clusters, please refer to the Replication and Remote Access Setup documentation.

Initiate Recovery

Cohesity offers flexible recovery options tailored to the user's needs, varying based on the protection type and the source system. For example, Cohesity supports file-level recovery, instant volume mounts, instant mass restores, bare metal recovery, and copy recovery. These recovery choices are influenced by key business drivers that shape the customer’s specific requirements.

For more information on Recovery, check Cohesity Documentation.

Quorum Approval

Quorum-controlled recovery is crucial in data protection as it ensures recovery actions are approved by a majority, minimizing risks, preventing unauthorized access, and maintaining data integrity during restoration. In a Cyber Recovery scenario, multiple teams—such as Data Protection, Security, IT, Legal, and Compliance—are involved. Implementing a quorum-controlled recovery ensures that all teams provide their approval and that the entire process undergoes a thorough review.

As a prerequisite, a quorum group is established with key stakeholders, specifying the minimum number of approvals required for the recovery request to proceed. When a recovery task is initiated, the action does not begin immediately; instead, a quorum approval request is sent to all stakeholders. Each stakeholder must then decide whether to approve or reject the request. Recovery only begins if the quorum approval is granted, reinforcing security and compliance throughout the process.

For further details on configuring and using quorum functionality, refer to the Quorum section in the Cohesity Documentation.

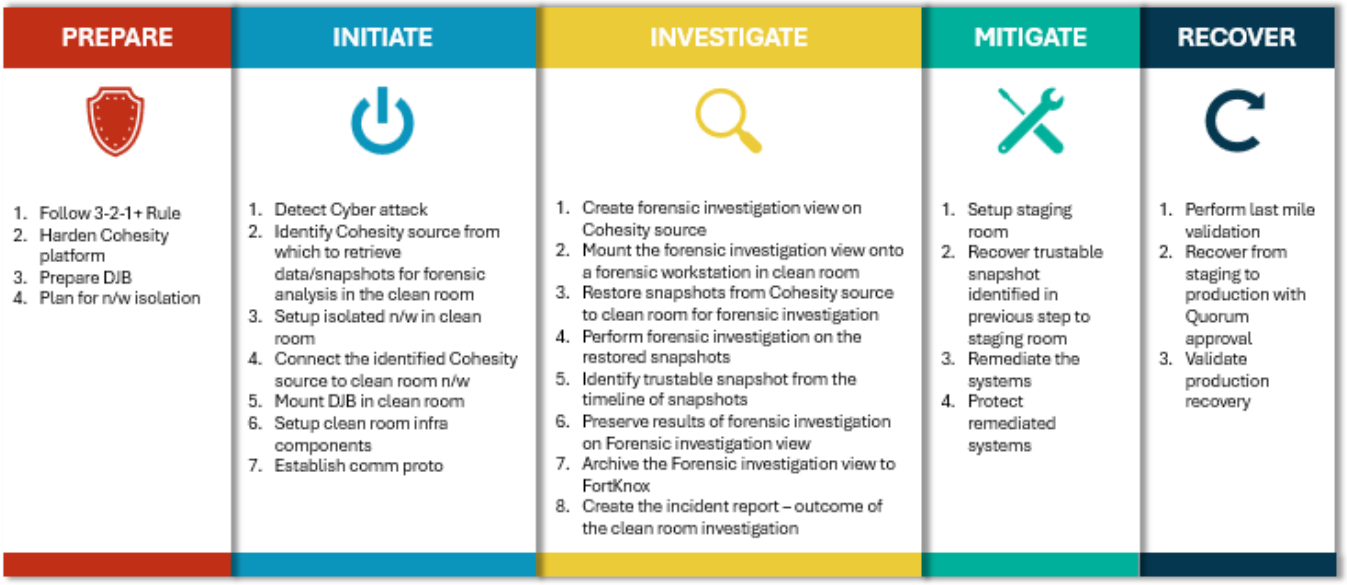
Validate Production Recovery

Once the quorum request is approved, the recovery of workloads to the production environment begins. You can monitor the progress of this recovery through the Cohesity user interface. After the recovery is complete, it is crucial to validate the recovered systems to confirm they are fully functional.

Summary

- **Consolidated Overview**: A one-page summary covering all sections for quick reference.

Figure 10: Cohesity Clean Room Solution Summary



Appendix

Register Source (vCenter)

Follow the steps below to register the vCenter Source:

1. Navigate to **Data Protection** > **Sources**.
2. Select **Register > Virtual Machines**.
3. Select a Hypervisor Source Type from the drop-down.
4. Enter the information for your source type and enable the option “Network for Data Transfer.” Enter the information of the subnet (isolated environment) and click **Register**.

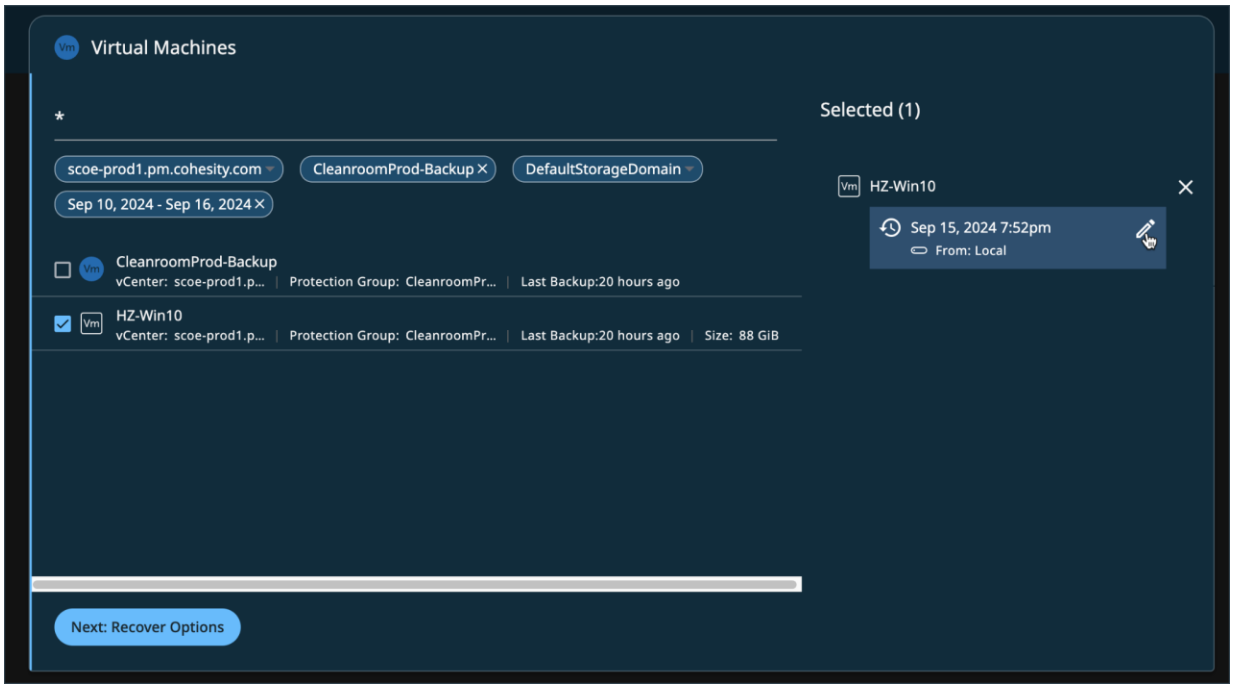
Follow the steps in Register or Edit a Hypervisor Source for more details.

Recover Older Snapshots

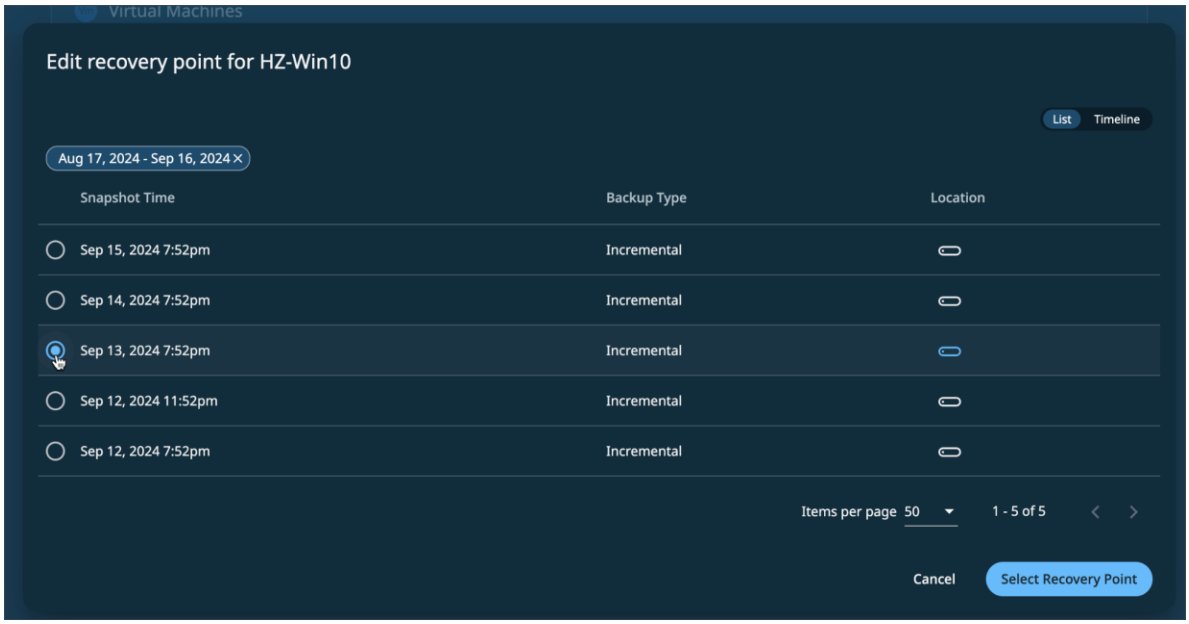
By default, the last snapshot is selected for recovery. If older snapshots need to be investigated or recovered from the Protection Group, traverse through the available snapshot list and recover the required snapshot.

Follow the steps below to recover from a different snapshot.

1. Hover the mouse over the snapshot from the selected list and click the edit icon.



2. From the list of snapshots, choose the snapshot to recover from. Click **Select Recovery Point**.



3. Follow the steps necessary to recover the VM, virtual disk, or mount the disk.

Recover from Customer Managed Cluster

File/Folder Recovery

Follow the below steps to recover files/folders to the target cluster

1. Navigate to **Data Protection** > **Recoveries**.
2. Click Recover and then select Files or Folders.
3. Browse and select the files and folder to recover.
4. In **Recover To**, select **New Server**. This is the clean room vCenter.
5. From the **Registered Source** drop-down menu, select clean room vCenter.
6. From the **Target** drop-down menu, select a VM to which the files and files will be recovered.
7. Select the **Restore Method**.
8. Click **Recover**.

By default, only the last snapshot is recovered. To recover previous snapshots, follow the steps in Recover Older Snapshots.

Refer to Recover Files or Folders to a New Location for more information.

Download Files/Folders

Follow the steps below to download the file/folder to the local system.

1. Navigate to **Data Protection** > **Recoveries**.
2. Click **Recover** and then select **Files or Folders**.
3. Browse and select the files and folder to download.
4. Click **Download Files**.

VM Recovery

Follow the steps below to recover the VM to the target cluster:

1. Navigate to **Data Protection** > **Recoveries**.
2. Click **Recover** > **Virtual Machines** > **VMs**.
3. Search and select the VMs to recover.
4. Select one or more VMs or Protection Groups containing the snapshots to recover.
5. Select the **New Location** to recover the VM to the clean room cluster.
6. Select the **Recovery Type, Copy, or Instant Recovery**, and click **Recover**.

By default, only the last snapshot is recovered. To recover previous snapshots, follow the steps in Recover Older Snapshots.

Refer to Recover VMs to a New Location for more information.

Virtual Disk Recovery

Follow the steps below to recover the virtual disk to the target cluster:

1. Navigate to **Data Protection** > **Recoveries**.
2. Click **Recover** > **Virtual Machines** > **Virtual Disks**.
3. Search and select the VM whose virtual disks you want to recover.
4. Recover to the New Location. Select the clean room cluster as the source and select the appropriate Target.
5. Select the virtual disk, the recovery type, and the datastore you want to recover to.
6. Click **Recover**.

By default, only the last snapshot is recovered. To recover previous snapshots, follow the steps in Recover Older Snapshots.

Refer to Recover Virtual Disks to a New Location for more information.

Instant Volume Mount

Follow the below steps to perform the Instant Volume Mount to the target VM:

1. Navigate to **Data Protection** > **Recoveries**.
2. Click **Recover** > **Virtual Machines** > **Instant Volume Mount**.
3. Search and select the server that contains the data you want to mount.
4. In the Recovery menu, select the volume that you want to mount.
5. From the Recover To options, select New Location, the clean room cluster.
6. Click **Recover**.

By default, only the last snapshot is recovered. To recover previous snapshots, follow the steps in Recover Older Snapshots.

Refer to Instant Volume Mount to a New Location for more information.

Recover from FortKnox

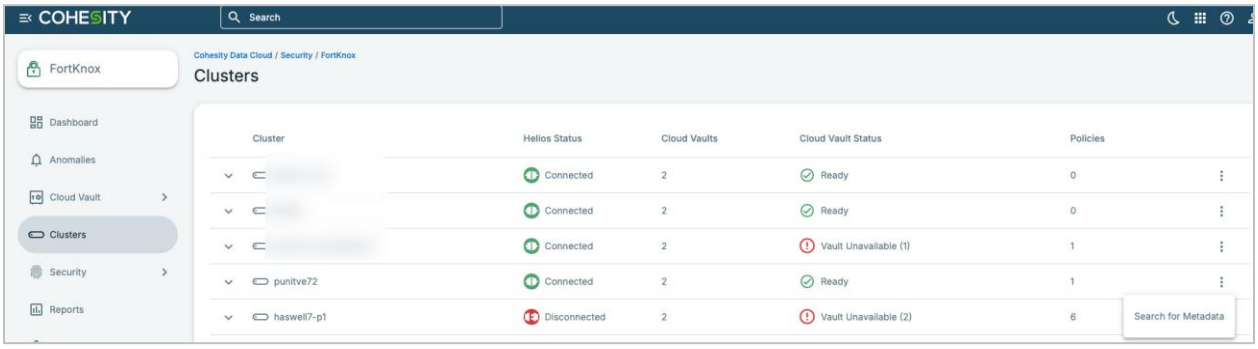
In a disaster, if you lose the connection to both primary and secondary clusters, you can retrieve your data (files/folders or VM) from FortKnox. The outline procedure for the recovery is as follows:

1. A standby Cohesity cluster with a Helios connection is required to retrieve the data from Fort Knox.
2. Retrieve the metadata from FortKnox for the primary cluster, which is no longer operational, and the standby Cohesity cluster.
3. Perform the recovery from the Cohesity Cluster.

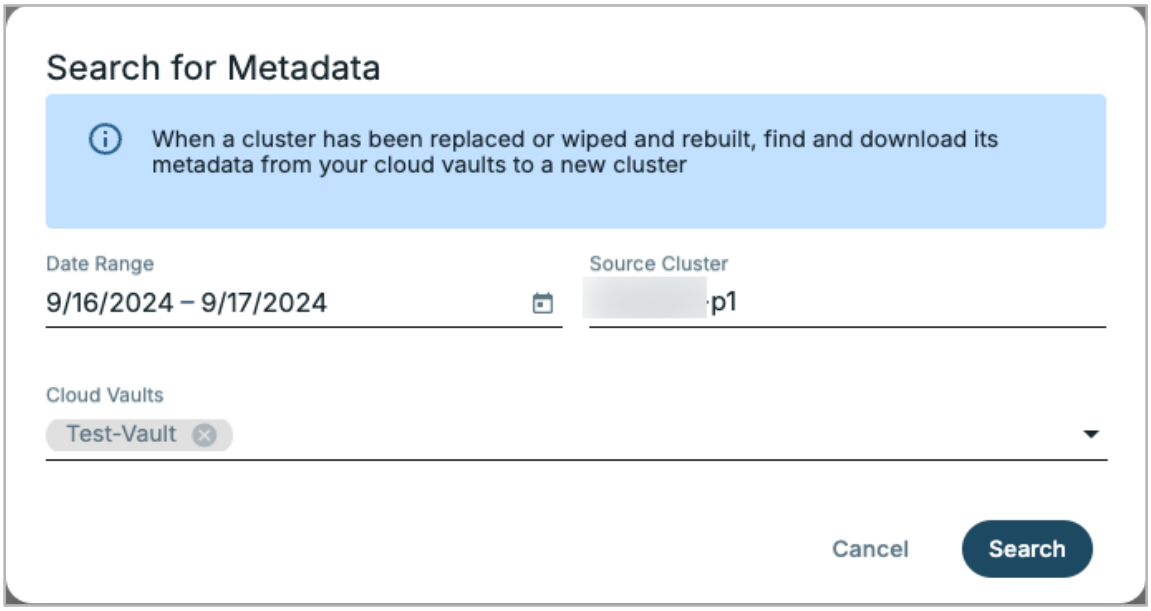
Download Metadata to Standby Cohesity Cluster

Follow the below steps to download metadata from the Primary/Secondary cluster to the standby cluster:

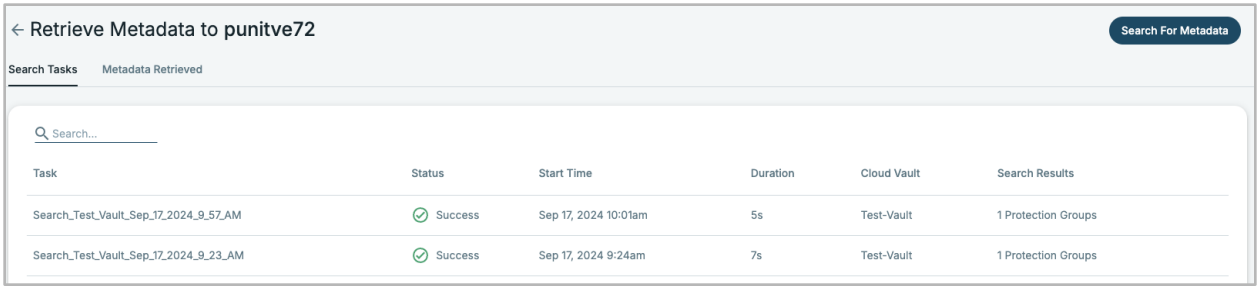
1. Login to Helios and click **Security** > **FortKnox**.
2. To retrieve the metadata of the primary/secondary cluster to the standby cluster, navigate to the **Clusters,** click on the three dots, and click **Search for Metadata** on the standby cluster.



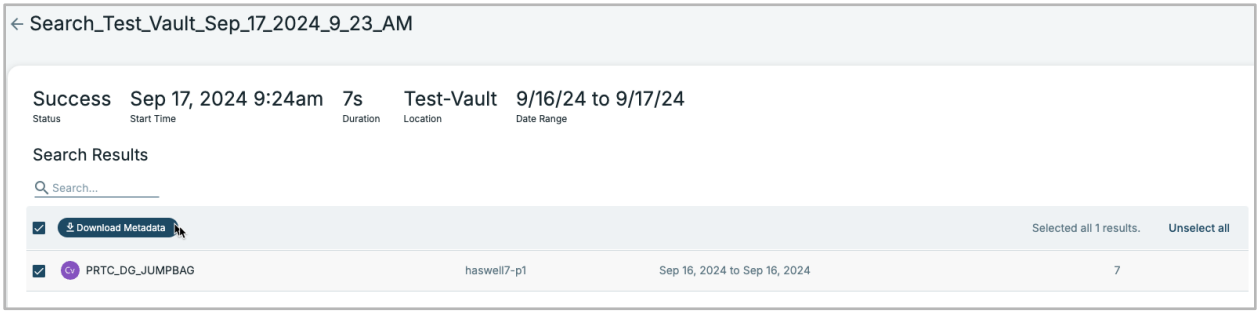
3. Enter the date range and source cluster for which you want to retrieve the metadata and cloud vaults. Click on Search.



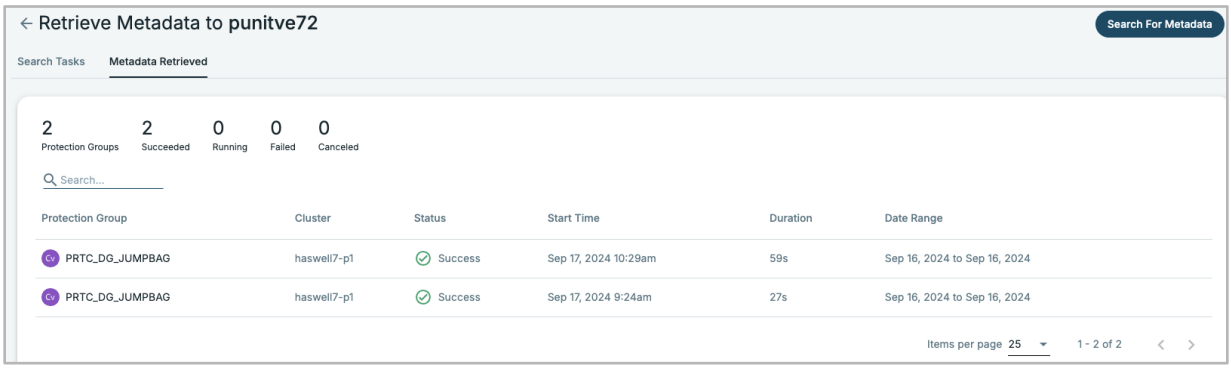
4. In case of quorum configuration, the request will be submitted for quorum approval. Once approved, the metadata search will start.



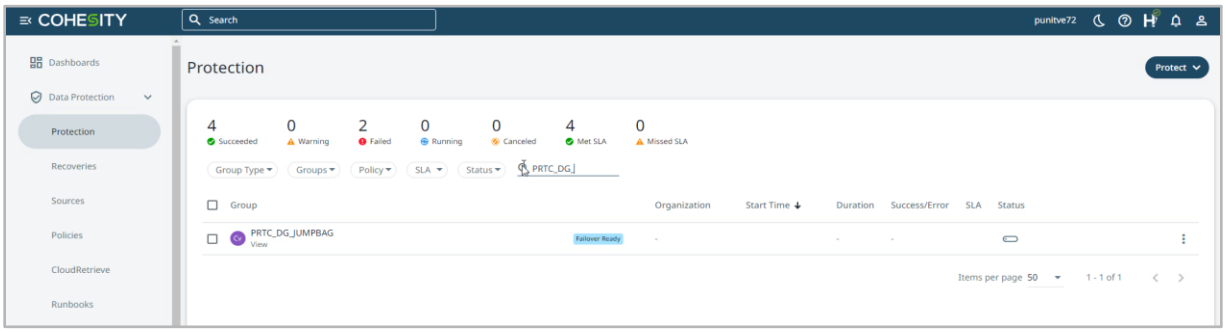
5. Once the search task is completed and the status is “Success,” click on the **Task** to reflect the protection group.



6. Select the protection group inside the search task and click on “**Download Metadata**.” The metadata will be downloaded to the standby cluster.



7. In the “**Metadata Retrieved**” section, monitor the download metadata task. Once the status changes to success, you can perform the **Failover** from the standby cluster.
8. On the standby cluster, navigate to **Data Protection** > **Protection** and search for the Protection Group. The Protection Group will be reflected as Failover Ready.



9. Perform the failover operation on the Protection Group.
10. Once the failover operation is complete, the recovery tasks can be performed on the Protection Group.

File/Folder Recovery

Follow the steps below to recover files and folders from FortKnox to the target cluster.

1. In FortKnox, navigate to **Data Protection** > Recoveries and select Recover
2. Go to **Virtual Machines** > **Files or Folders**.
3. The Select Cluster page is displayed. Select the source VM cluster.
4. Browse and select the files and folder to recover.
5. In **Recover To**, select **New Server**. This is the clean room vCenter.
6. From the Registered Source drop-down menu, select clean room vCenter.

7. From the Target drop-down menu, select a VM to which the files and files will be recovered.
8. Select the Restore Method.
9. Click **Recover**.

Refer to Recover VMware Files or Folders to a New Server for more information.

Download File/Folder

Follow the steps below to download the file/folder to the local system.

1. In FortKnox, navigate to **Data Protection** > Recoveries and select Recover.
2. Click **Recover** and then select **Files or Folders**.
3. Browse and select the files and folder to download.
4. Click Download Files.

VM Recovery

Follow the steps below to recover VMs from FortKnox to the target cluster.

1. In FortKnox, navigate to **Data Protection** > **Recoveries** and select **Recover.**
2. Go to **Virtual Machines** > **VMs**.
3. The Select Cluster page is displayed. Select the source VM cluster.
4. Search and select the VMs to recover.
5. Select one or more VMs or Protection Groups containing the snapshots to recover.
6. Select the New Location to recover the VM to the clean room cluster. Provide the clean room cluster details and resources.
7. Modify the Recovery options as required.
8. Select the Recovery Type, Copy, or Instant Recovery, and click **Recover**.

Refer to Recover VMware VMs to a New Location for more information.

Virtual Disk Recovery

Follow the steps below to recover the virtual disk from FortKnox to the target cluster.

1. In FortKnox, navigate to **Data Protect** > **Recoveries** and select Recover.
2. Go to **Virtual Machines** > **Virtual Disks**.
3. The Select Cluster page is displayed. Select the source VM cluster.
4. Search and select the VM whose virtual disks you want to recover.

5. Recover to the New Location. Select the clean room cluster as the source and select the appropriate Target.
6. Select the virtual disk, the recovery type, and the datastore you want to recover to.
7. Click **Recover**.

Refer to Recover VMware VM Virtual Disks for more information.

Instant Volume Mount

Follow the steps below to perform the Instant Volume Mount to the target VM:

1. In FortKnox, navigate to **Data Protect** > **Recoveries** and select **Recover**.
2. Go to **Virtual Machines** > **Instant Volume Mount**.
3. The Select Cluster page is displayed. Select the source VM cluster.
4. Search and select the server that contains the data you want to mount.
5. In the Recovery menu, select the volume that you want to mount.
6. From the Recover To options, select New Location, the clean room cluster.
7. Click **Recover**.

Refer to Instant Volume Mount to a New Location for more information.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

- Karthick Radhakrishnan is the Director of the Security Center of Excellence, where he leads the development and management of Cohesity Security solutions and integrations.
- Punit Gupta, Staff Technical Solution Engineer – Focuses on data protection, physical agents, SmartFiles, Multitenancy and Cohesity storage as a backup target
- Shashank SR, Staff Technical Solution Engineer – Focuses on Cohesity BaaS, M365 Protection and Gaia.
- Surya Swaminathan, Sr Technical Solution Engineer – Focuses on DataHawk and FortKnox.

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	Aug 2025	Republished with latest template
1.1	Nov 2024	Glossary (Clean Room) Updates
1.0	Oct 2024	First full 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.