COHESITY

Version 1.0

July 2021

Bare Machine Recovery for Linux Using Cohesity & Cristie

Use Cristie BMR with Cohesity to Recover Your Linux System

ABSTRACT

Physical Server backup and recovery entails challenges because servers contain user directories and system directories to restore in ways specific to the operating system. Cohesity's approach for physical server recovery using the Cristie BMR software provides the best solution for performing physical server backups of both user and system files and subsequent recovery, either into the same server or an entirely new server. Cohesity ensures the protection and recovery of the server.

Table of Contents

Figures

Tables

The Need for Bare Machine Recovery

Because many of today's organizations leverage physical server infrastructure for their most critical workloads, they require enterprise-level data protection solutions. Protecting a server, be it physical or virtual, with a Bare Machine Recovery (BMR) solution has always been challenging because the vendor landscape has many players with varying capabilities and support structures. Only a few key players provide an end-to-end solution.

A good BMR solution makes it seamless for the user to recover servers into a new machine where they do not see a difference between the old machine and the recovered machine. There are several factors to consider when evaluating and selecting the best BMR solution for your infrastructure:

- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)
- Simplicity of the solution
- Your organization's data protection & disaster recovery strategies
- Heterogeneous operating system support
- Integrity and reliability of the recovered system
- Platform-agnostic support

NOTE: The scope of this guide is limited to Bare Machine Recovery of physical and virtual Linux servers that have the Cohesity Agent for Linux installed.

Cohesity has partnered with Cristie Software, a leading provider of BMR, to provide a comprehensive backup and recovery solution for servers. Achieving your recovery objectives is now more straightforward with Cohesity. While Cristie's Bare Machine Recovery (CBMR) software enables you to extract and bundle your system data files, Cohesity works with CBMR to back up all the mounted filesystems. Using CBMR with Cohesity helps backup administrators to back up and restore the operating system with all the file mounts while preserving the state of the applications running on that system.

This solution guide details the steps and best practices for backup administrators to set up, schedule, and manage bare machine restores of Linux servers using CBMR software with Cohesity, as well as several recovery scenarios.

Benefits of Using BMR with Cohesity

Cohesity's BMR solution is built to consolidate and integrate all the backup and recovery capabilities onto one simple to manage platform. For BMR, Cohesity integration with CBMR facilitates automatic backups and accelerated recovery of servers directly from backups.

Cohesity's partnership with CBMR enables enterprises to:

- **Restore Servers Quickly**. Boot from a preconfigured Linux ISO image to start the recovery process. Bootstrapping from an ISO eliminates the overhead of installing an operating system before launching your server recovery.

- **Leverage Flexible Bare Machine Recoveries**. Use a single platform to protect servers and restore them to their original state on the same or dissimilar hardware. This process is flexible and gives you the option to restore a physical server on its original hardware (P2P), migrate a physical server to another physical server (P2P), recover a physical server as a VM (P2V), or recover a VM as a VM (V2V). For more, see Recovery Strategies with Cristie BMR below.
- **Simplify the Workflow**. Use a single, unified window to schedule backups, monitor progress, and initiate point-in-time restores.
- **Storage-efficient Backups.** Organize your backups into two types: physical server backups and BMR-specific backups. Then use Cohesity's advanced algorithms for compression and deduplication to dramatically reduce storage consumption and lower protection costs.
- **Secure Data**. Cohesity employs both in-flight and at-rest encryption based on the solid AES-256 CBC (Cipher Block Chaining) encryption standard.

Terminology

Several concepts and terms are essential to understand as you learn about Cohesity's data protection solution for servers.

Table 1: Terminology for BMR with Cohesity

TERM	DEFINITION
Cristie BMR (CBMR)	The CBMR software enables server recovery onto a bare machine.
Cristie ISO	A pre-created ISO is available for download from Cristie. The Cristie ISO is required to load the CBMR recovery environment.
IPMI	Intelligent Platform Management Interface that is used to monitor and manage a server, including access to the server's console remotely.

Understand BMR with Cohesity

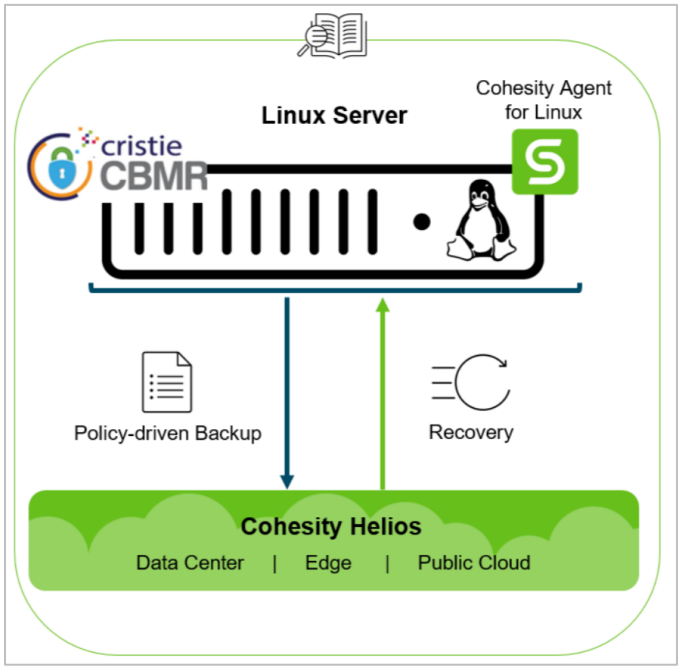
To protect your server for bare machine recovery, you need to back up both the machine configuration and the data. In our solution, install CBMR on the server that you need to protect to back up all the mounted filesystems. Install the Cohesity Agent for Linux on the same server, which facilitates communication between the Linux machine and Cohesity. This allows you to back up the entire server using a single Cohesity Protection Policy.

When you set up protection for your server, you create two schedules in the same Protection Policy: one for backing up the volume data and another less frequent schedule for BMR protection.

When the data protection schedule triggers a backup for the first time, it backs up all your data, that is, it creates a full backup. Subsequent scheduled runs will only capture data that has changed, that is, they create incremental backups.

When Cohesity triggers CBMR to back up all the file mounts, it runs a full backup each time. We recommend a less frequent schedule for the BMR backup since the system data files' change rate is low compared to an application or a database.

Figure 1: Protect Your Server for Bare Machine Recovery



Recovery Strategies with Cristie BMR

Planning for disaster recovery is a vital part of any company’s infrastructure strategy. A robust disaster recovery strategy outlines how quickly organizations restore systems from a potential failure. The magnitude of losses can range from an OS or disk failure to a state where a complete reconstruction of infrastructure is required. Some scenarios that can require the rebuilding of your entire infrastructure include:

- Ransomware & malware attacks

- Damage to the hardware
- Datacenter outage due to natural calamity
- Migrating to an environment that runs on dissimilar hardware

Bare machine recovery is suitable in scenarios where there is a need to efficiently rebuild your infrastructure . With Cohesity and CBMR integration, you can take advantage of the Cohesity agent for Linux and the recovery ISO for a tried-and-tested disaster recovery solution. By creating a Virtual Tape Drive (.vtd) file with all the volume and system data and creating a bootable environment, the entire recovery process is made simple, reliable, and fast.

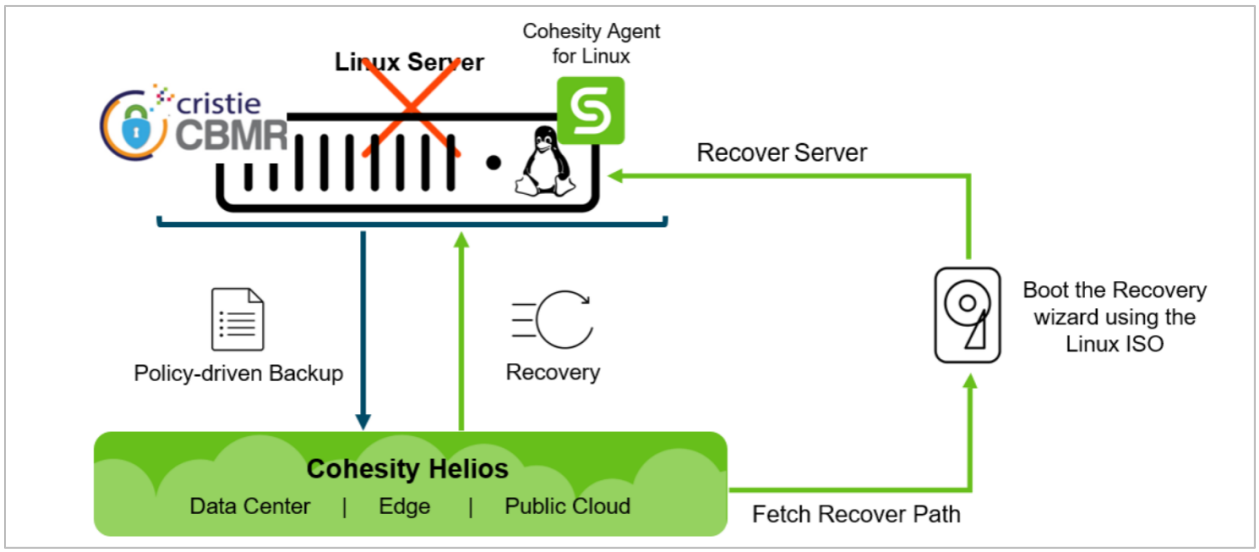
To mitigate data loss in the event of a failure, we need to be prepared . Let's discuss three such recovery scenarios.

NOTE: The recovery steps for all the scenarios described below are the same. Find those steps in the Set Up BMR with Cohesity chapter.

Recover Server to Original Machine (P2P)

In case a malware attack or a fat finger error deletes all the data on your server (including system files) or makes your data inaccessible, but the server remains accessible, you can recover the system back to a stable state on the original machine using CBMR on Cohesity.

Figure 2: P2P Workflow — Recover Server to Original Machine

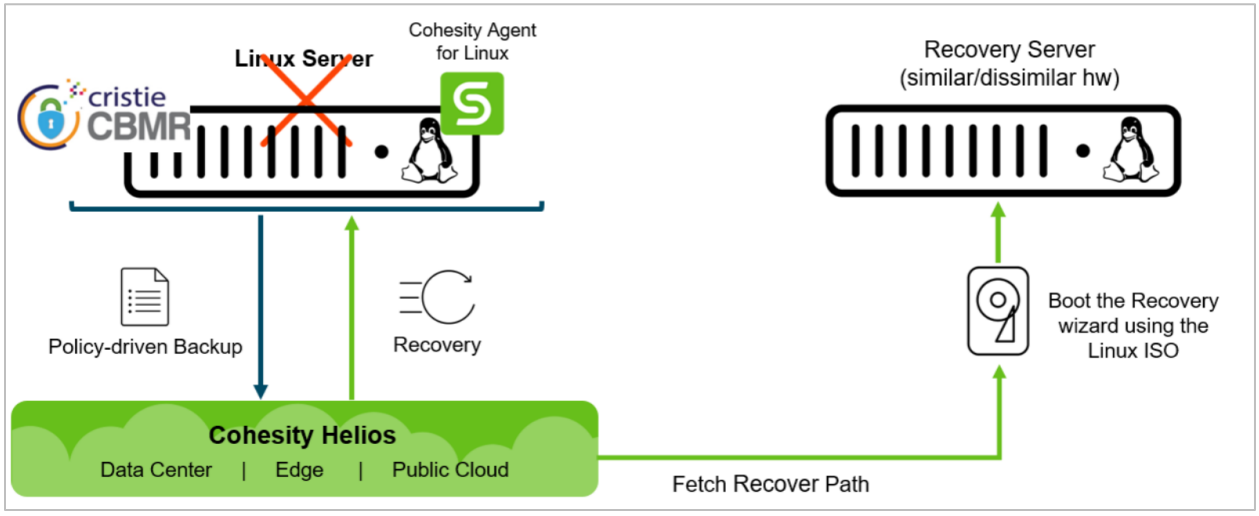


Recover Server to New Machine (P2P)

With CBMR backups in Cohesity, you can recover your server on the same or dissimilar hardware. Recovery to a new machine is crucial if your server becomes unavailable due to a complete hardware failure and is also helpful as a data-migration strategy where you restore the server onto a new (similar or dissimilar) machine.

Additionally, organizations can plan their periodic DR testing to a new (similar or dissimilar) machine.

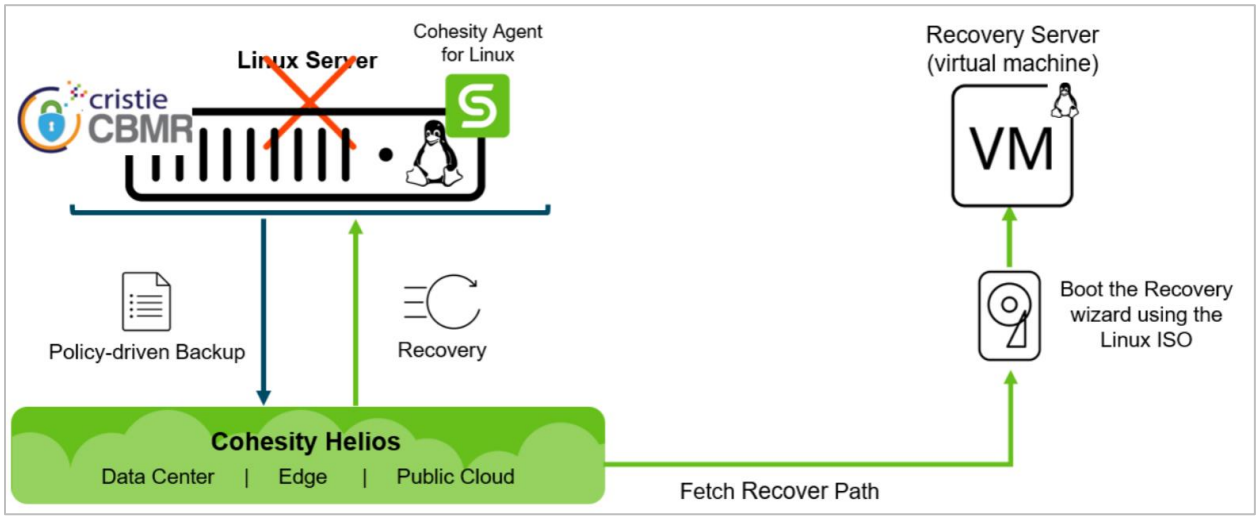
Figure 3: P2P Workflow — Recover Server to New Machine



Recover Server as a VM (P2V)

If your physical server becomes unavailable due to a hardware failure, you can also restore the physical server as a virtual machine (VM). This approach is also helpful in dev/test use cases where you periodically need to restore physical servers as VMs.

Figure 4: P2V Workflow — Recover Server as a Virtual Machine



Recover VM as VM (V2V)

You can also protect a VM by deploying a Cohesity Agent and CBMR and recovering your protected VM. However, VMware's native recovery method is more effective in this scenario.

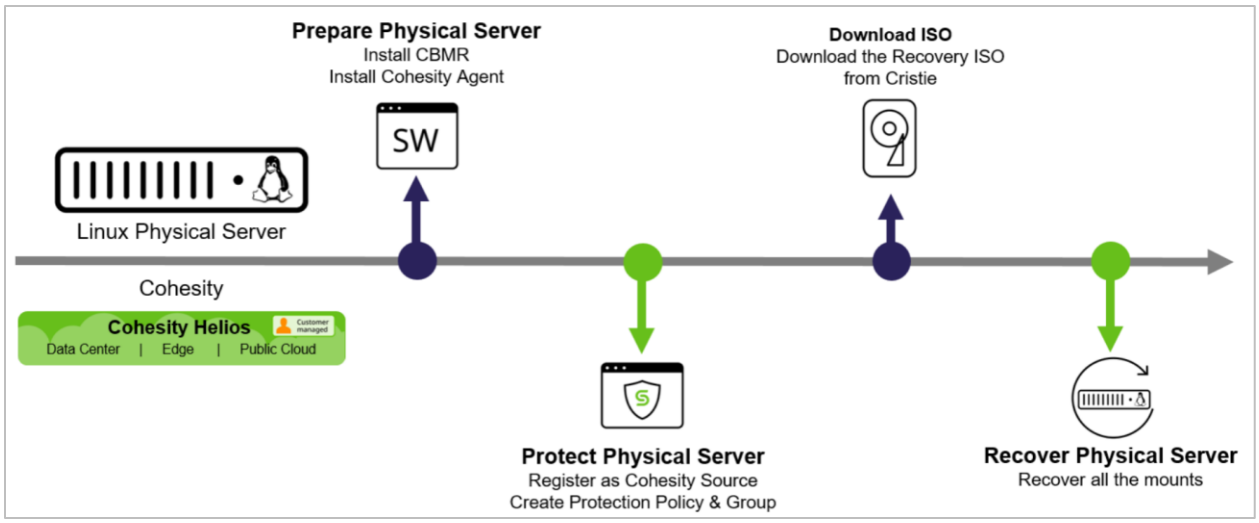
Set Up BMR with Cohesity

The first thing to do is install CBMR and set it up to protect your server with Cohesity.

To set up and start using CBMR with Cohesity, complete the following tasks:

1. Prepare the physical server for Cristie-Cohesity integration.
2. Register your server as a Cohesity source and set up protection.
3. Download the recovery ISO from Cristie.
4. Recover your server using Cohesity and CBMR.

Figure 5: Cohesity with Cristie BMR Solution Workflow



NOTE: Before you begin configuring BMR, see the list of supported workflows

Prepare the Server for Cristie-Cohesity Integration

CBMR comes with a licensed BMR software suite, and the software needs to be running on the server marked for protection. This software runs as a deployment service and coordinates backups with the Cohesity agent for Linux that must be running on the same server.

To set up your server for BMR protection:

1. Install CBMR.
2. Install the Cohesity Agent for Linux on the same server.

Install CBMR

Start by installing Cristie's Bare Machine Recovery software. For that, you'll need:

- A server running a supported Linux OS. See **Physical Servers** in the Supported Software list for Cohesity-qualified versions. For a list of Cristie-supported OS versions, see the Product Support section in this Cristie BMR page.
- Login credentials with root/sudo for the user on the Linux server.

  NOTE: The CBMR application requires access to all the OS for backup.

- A licensed version of the qualified CBMR Suite. For Cohesity-qualified CBMR agent versions, see Cristie BMR in the Supported Software list.

To install CBMR:

1. Download your licensed CBMR installation binary and copy the installation file to a temporary location, for example, '/tmp.'
2. The CBMR installation binaries are available in three formats: RPM package, Debian package, and Tar file.
3. To install CBMR from an RPM package, run the "***rpm -ivh --nodeps***" command.

   Example:

   ```
   rpm -ivh --nodeps cbmr-8.7.1008-1.x86_64.rpm
   ```

4. To install CBMR from a Debian package, run the ***dpkg*** command.

   Example:

   ```
   dpkg -i cbmr-8.7.1008-1_amd64.rpm
   ```

5. To install CBMR from a Tar file:

   a. Extract the Tar file using "tar xvzf" command

      Example:

      ```
      tar xvzf cbmr-8.7.1008-1.linux.x86_64.tar.gz
      ```

   b. Navigate to the extracted folder.

c. Run install to begin the installation

Example:

```
./install
```

6. Check the status of the installation in the "***/CBMRCFG/cbmrcfg.log***" file.
7. Once the installation is complete, run the ***licmgr*** command to check the license and validate the CBMR installation.

   Example:

```
licmgr -p cbmr
```

8. The next step is to copy the ***ubax_monitor*** file inside the tar package to /usr/bin to monitor the BMR protection status from the Cohesity user interface.

   Example:

```
# cd cbmr
cbmr]# cp ubax_monitor /usr/bin
```

IMPORTANT: Remember to register with Cristie and activate your Cristie license before your fully functional 30-day trial period expires.

For more, see CBMR Installation & License Guide For Linux in the Cristie documentation.

Install the Cohesity Agent for Linux

The Cohesity Agent for Linux helps establish the network path between the system image backup and Cohesity. The agent integrates with CBMR for scheduling BMR backups.

For instructions, see Install and Manage the Agent on Linux Servers in the online Help.

Protect Your Linux Server

Protecting your Linux server with Cohesity and CBMR involves two protection schedules. First, with frequent protection runs for the data, and second, for less frequent protection runs to save your machine's configuration. This prepares the configuration for the eventual need to restore the server onto the original or a dissimilar hardware.

Once you register your Linux server as a Cohesity source, you'll need to create a Protection Policy to schedule protection runs for both the volumes (data) and the BMR runs. Finally, you'll create a Protection Group, enable the option to include BMR backups, and add the Policy you created to schedule the protection runs. Setting the BMR option in your Protection Group allows the Cohesity agent for Linux to work in conjunction with CBMR to protect the servers.

IMPORTANT: Contact Cohesity Support to complete this configuration step before you start protecting your Linux Server.

Register Your Server as a Cohesity Source

The first step in protecting your server is to register it as a Cohesity source. For instructions to register a source with Cohesity, see Register or Edit a Physical Server in the online Help.

NOTE: While Cohesity supports registering a physical server with its FQDN (fully qualified domain name) *or* its IP address, the best practice is to use the FQDN. Using FQDN helps you avoid re-registering the server if the IP address changes.

After you register a source, navigate to **Data Protection** > **Sources** to confirm that it appears on the **Sources** summary page.

Create a Protection Policy

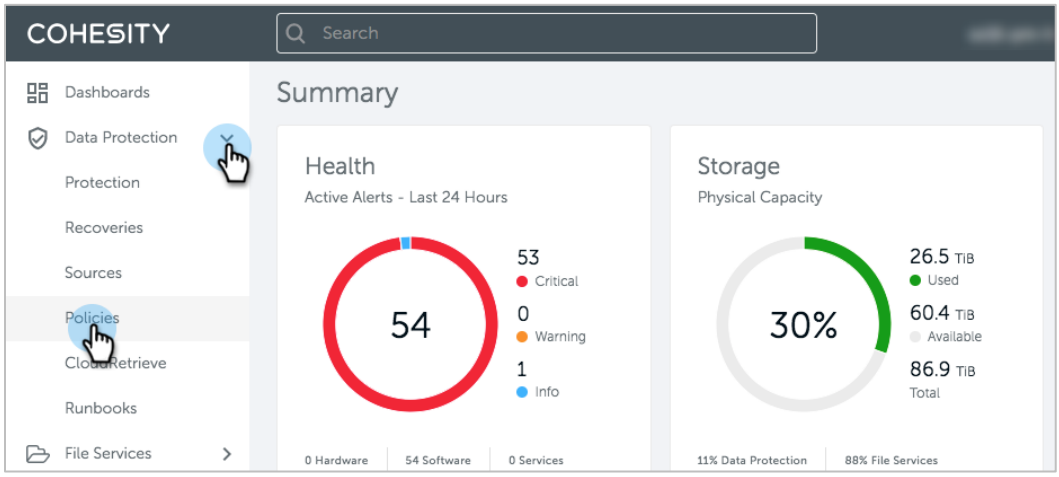
In Cohesity, Protection Groups use Protection Policies. Protection Policies reflect *business* needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). A Protection Group defines *operational* requirements, such as which source objects to protect, the Protection Policy to use, and operational considerations like indexing, exclusions and inclusions, alerts, app consistency, and more. This process of combining business needs (Policy) with the objects to protect (source data) and the operational requirements (Group) provides rich flexibility to customers.

A Protection Policy defines:

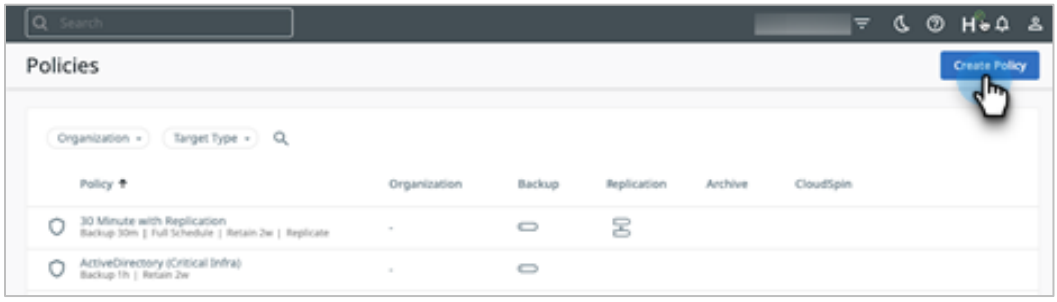
- How source data (like virtual & physical servers) is protected (backup, replication, and/or archival).
- The frequency of protection runs.
- Where the data is stored.
- How long the backed-up data is retained.

To create a BMR-enabled Protection Policy:

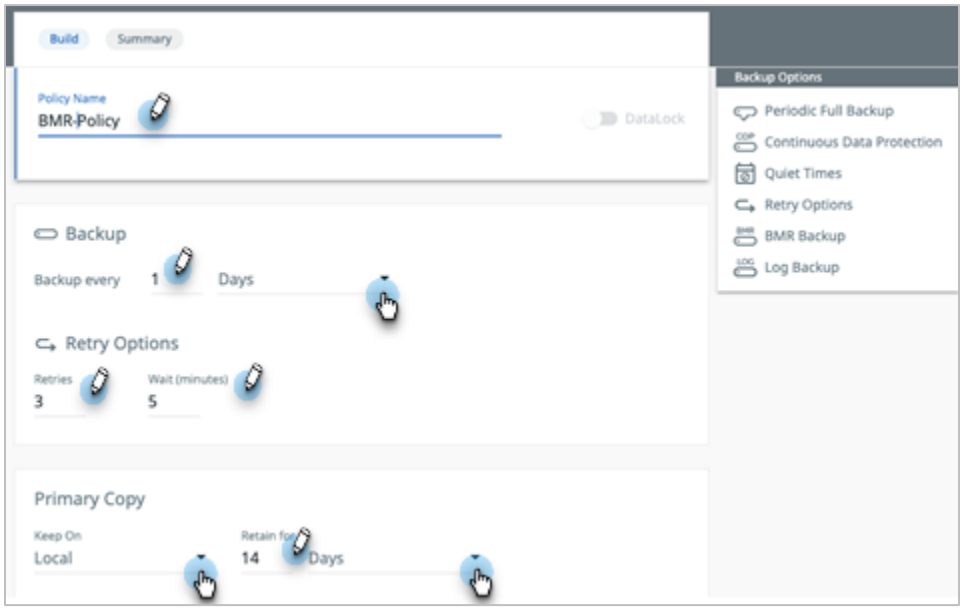
1. Log in to Cohesity.
2. Navigate to **Data Protection** > **Policies**.



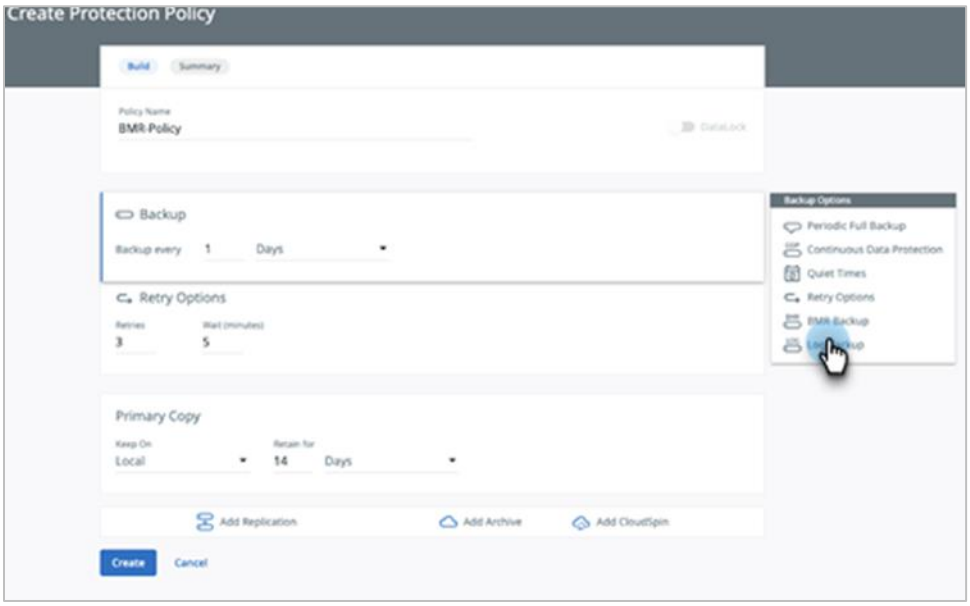
3. Click **Create Policy**.



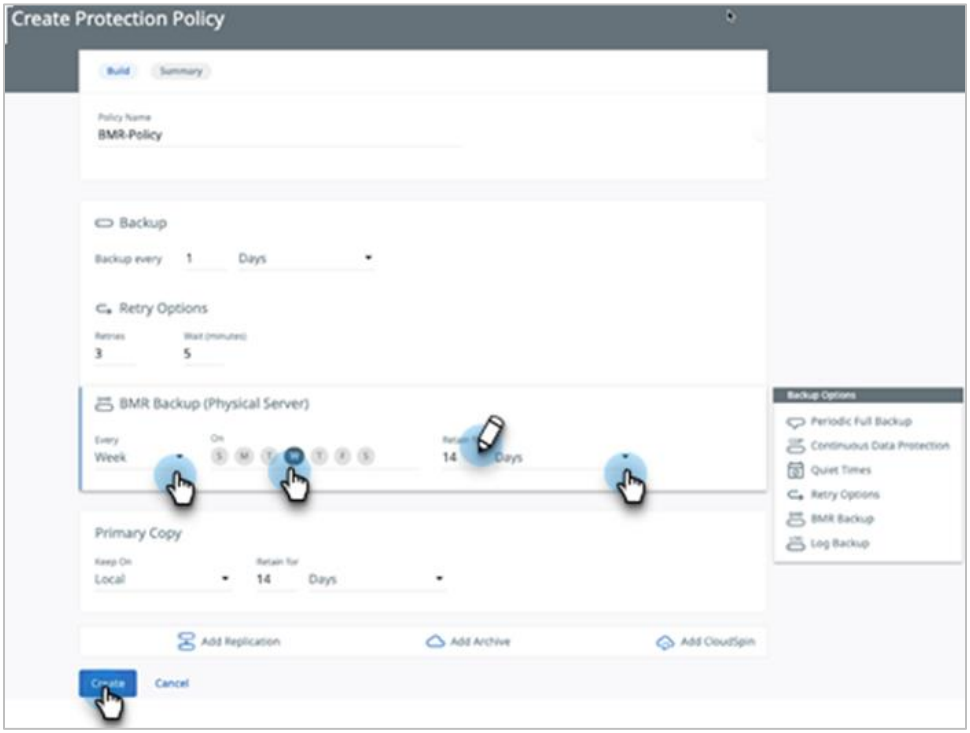
4. In the **Create Policy** form, enter a **Policy Name**, select the interval and retention times for the **Backup** for the data (volumes) on your server, edit the **Retry Options** if necessary, and specify the location (**Local**) to store the Primary Copy.



5. Click **BMR Backup** from the menu on the right to add a BMR Backup to the Policy.



6. Under **BMR Backup (Physical Server)**, set the **Create** frequency and day, and adjust the **Retain** period. Then click **Create**.



For more details, see Create or Edit a Standard Policy in the online Help.

Create Protection Group

Protection Groups combine operational requirements with the business requirements defined in a Protection Policy. Multiple Protection Groups can use the same Protection Policy, but each group can

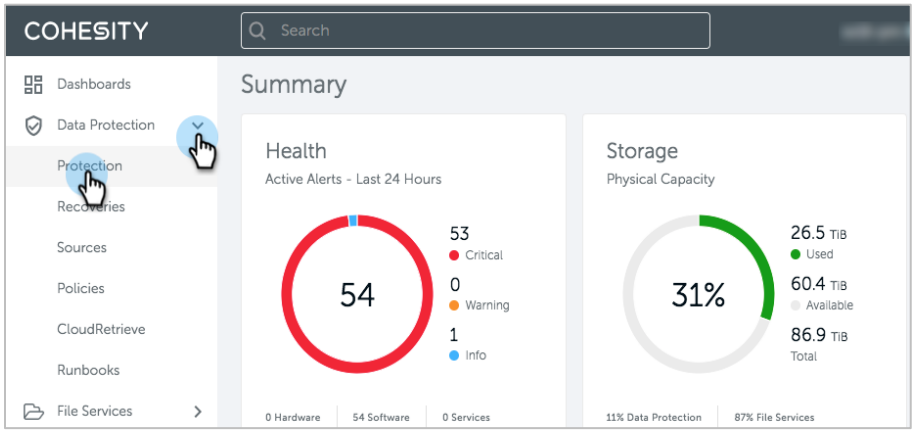
have only one policy. Protection Groups protect specific source objects, such as virtual servers, physical servers, views, SQL servers, Oracle databases, remote adapters, pure storage volumes, or network-attached storage (NAS).

The process to create a BMR-specific Protection Group is very similar to steps involved in protecting other sources except for an additional step to enable BMR backups. The steps to enable BMR backups are elaborated below.

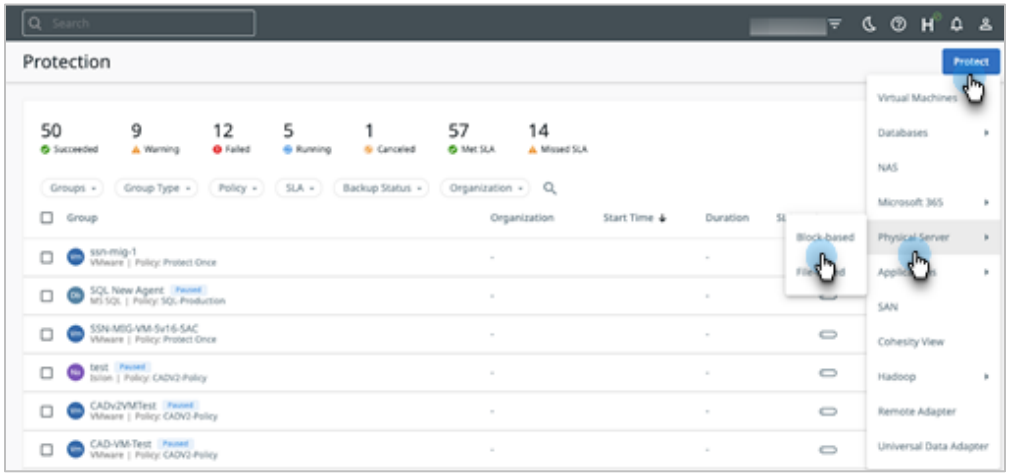
NOTE: Validate if you completed this configuration step before you configure protection for your Linux Server.

To create a BMR-enabled Protection Group for your server(s):

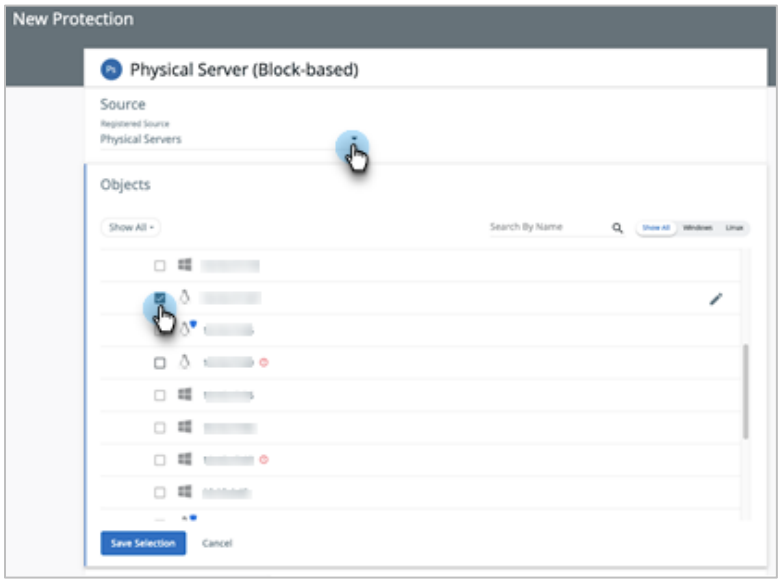
1. Navigate to **Data Protection** > **Protection**.



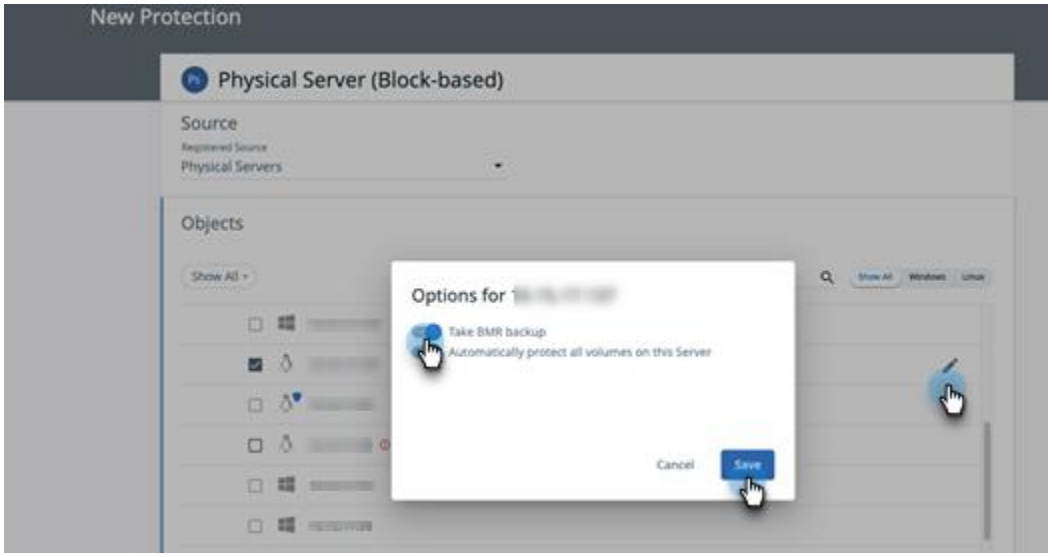
2. Click **Protect** and select **Physical Server** > **Block-based**.



3. In the **New Protection** form, select **Physical Servers** for **Source** and choose the specific servers you wish to protect.

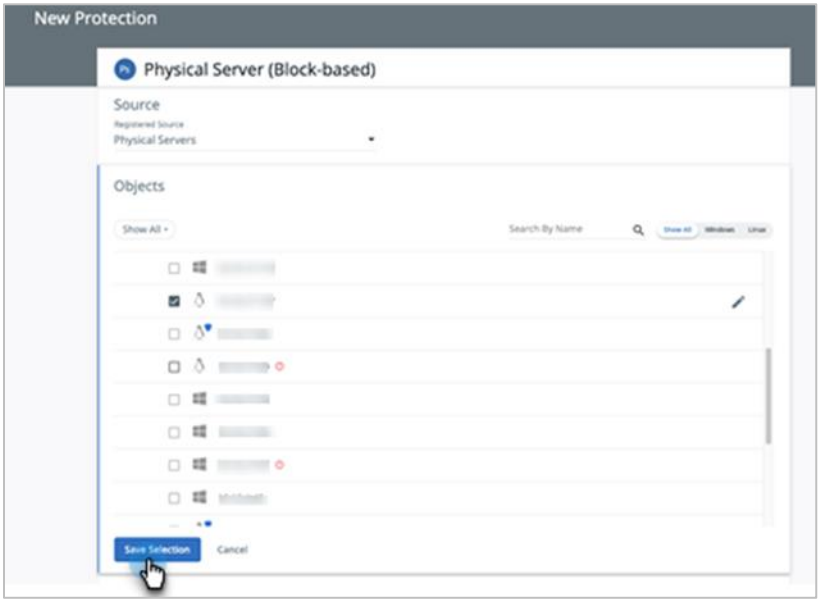


4. For each selected object, click the **Edit** button on the right, select **Take BMR backup** in the dialog, and click **Save**.

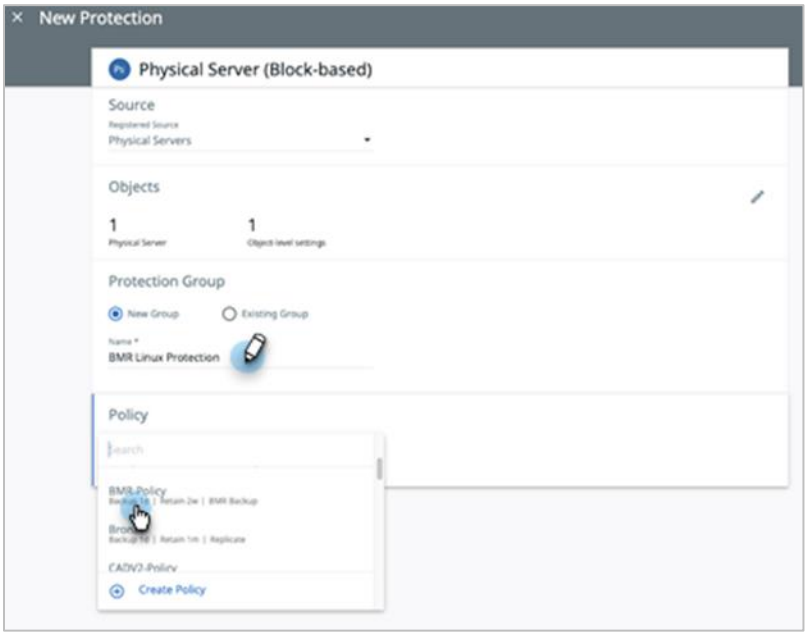


This step enables the Cohesity Agent for Linux to coordinate the entire physical server backup with the CBMR deployment service on the physical server.

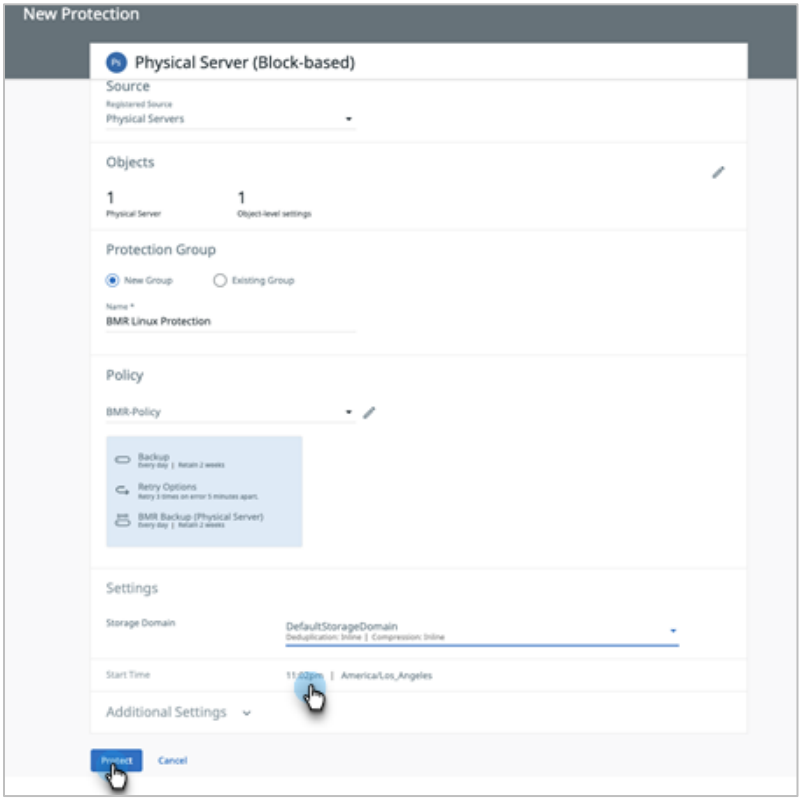
5. Once you have added the BMR backup to your source(s), click **Save Selection**.



6. Enter a **Group Name** and select the Policy you created earlier.



7. Select a **Storage Domain**, edit the **Start Time** if necessary, and click **Protect**.



For more details, including the **Additional Settings** in a Protection Group, see Add or Edit a Protection Group for Physical Servers in the online Help.

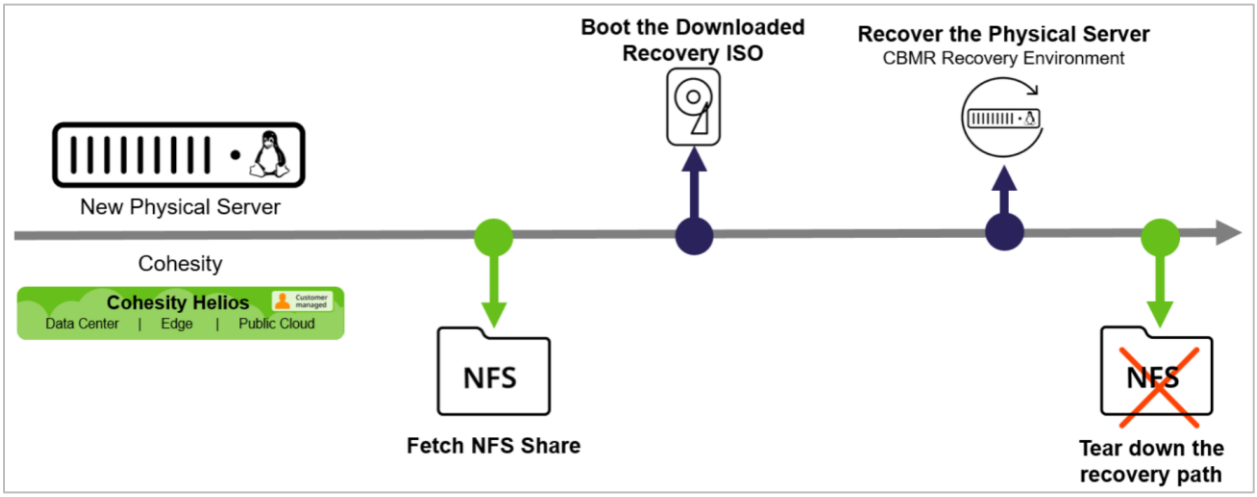
Recover Your Server Using Cohesity with CBMR

Cohesity facilitates the recovery of BMR backups, to both the original and alternate machines, at various degrees of granularity. During a BMR-enabled backup, all the mounted filesystems are copied to Cohesity as Virtual Tape Driver (.vtd) files to provide a seamless restore experience to the user. For a BMR recovery, the desired point-in-time state of the server is exposed as an NFS share. This NFS share is mounted while booting the recovery ISO to perform restoration of all the mounted filesystems. The restore process is hassle-free and automatic and it does not compromise the integrity of the server. You need not install the OS or manually partition the disk.

Recovering your server involves the following tasks :

1. Fetch the NFS share from Cohesity.
2. Boot the recovery ISO.
3. Recover your server using the CBMR Recovery Environment.
4. Tear down the recovery Path after completing the recovery.

Figure 6: Recover Your Server using Cohesity with CBMR



IMPORTANT: For a smooth recovery process, before you start, ensure that:

The IP address of the machine you are recovering onto is allowlisted in Cohesity.

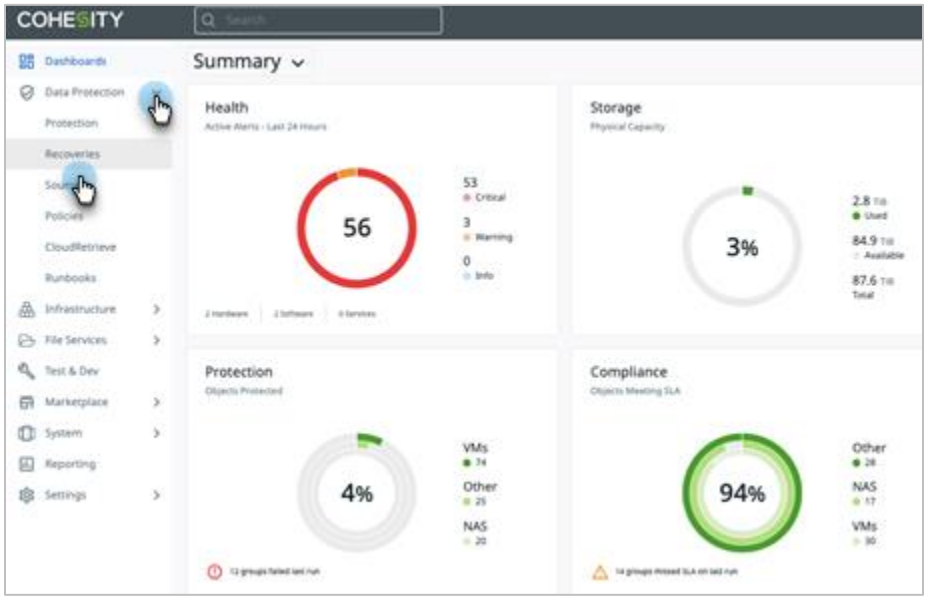
Fetch the NFS Share from Cohesity

To start the recovery process, you'll need to fetch the complete NFS share from Cohesity. Fetching this NFS share is a two-step process.

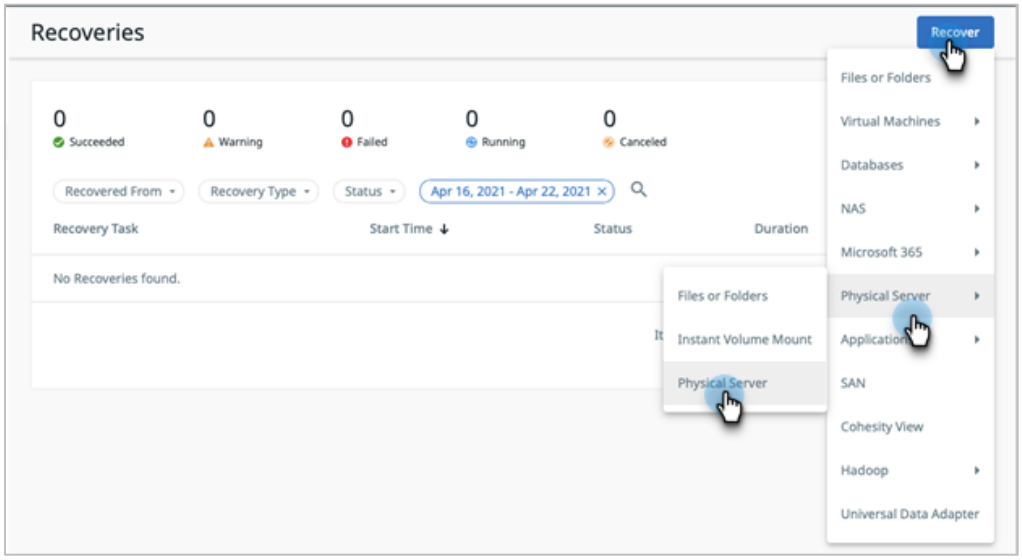
1. Get the unique recovery path that reveals the folder information.
2. Mount the unique recovery path temporarily to validate the recovery path that the recovery ISO will use.

To fetch the unique NFS share path for a bare machine recovery from Cohesity:

1. Log in to Cohesity.
2. Navigate to **Data Protection > Recoveries**.

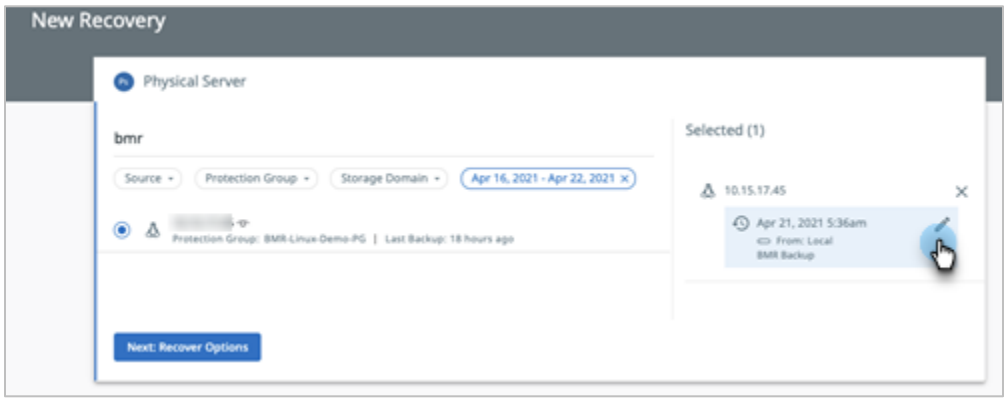


3. Select **Recover** > **Physical Server** > **Physical Server**.

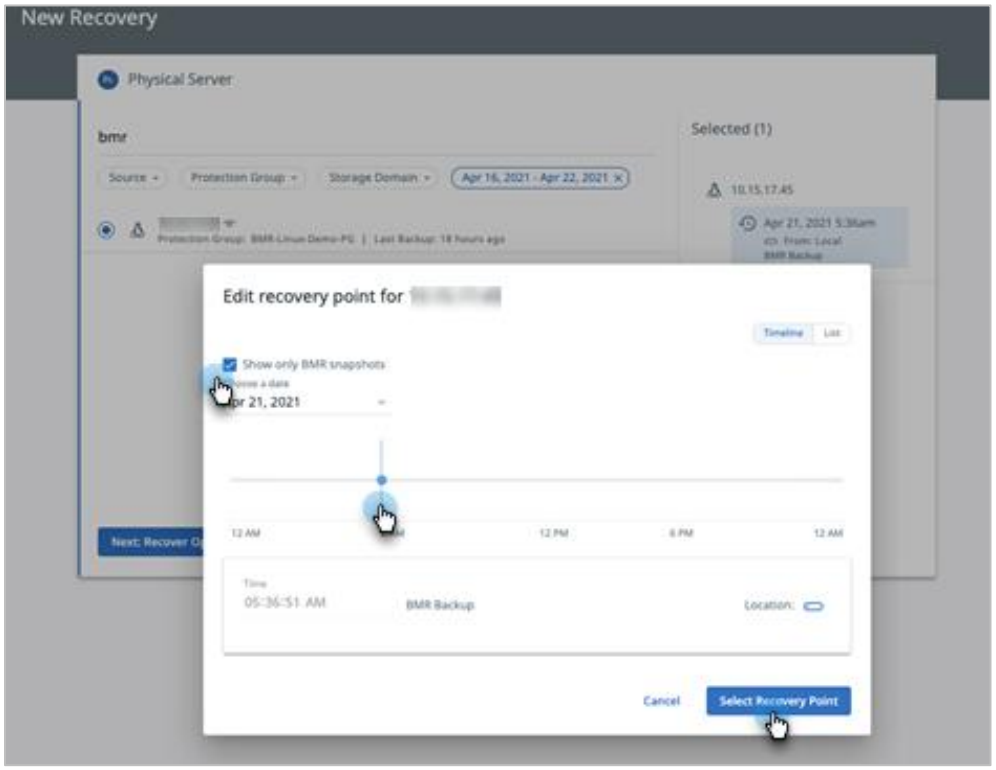


4. Enter a term to search by **Server or Protection Group Name**. In the search results, click the server you wish to recover.

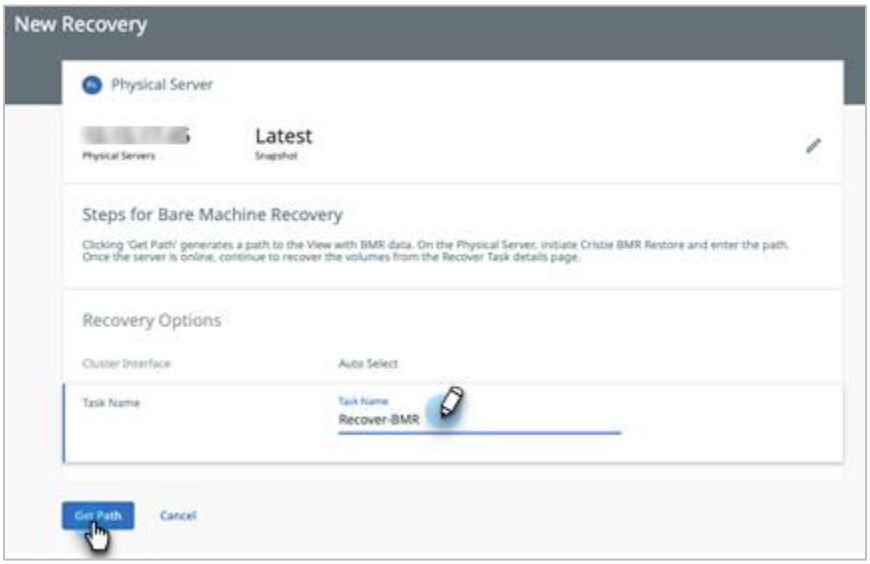
5. Select the BMR Recover Point, click the **Edit** (pencil) icon.



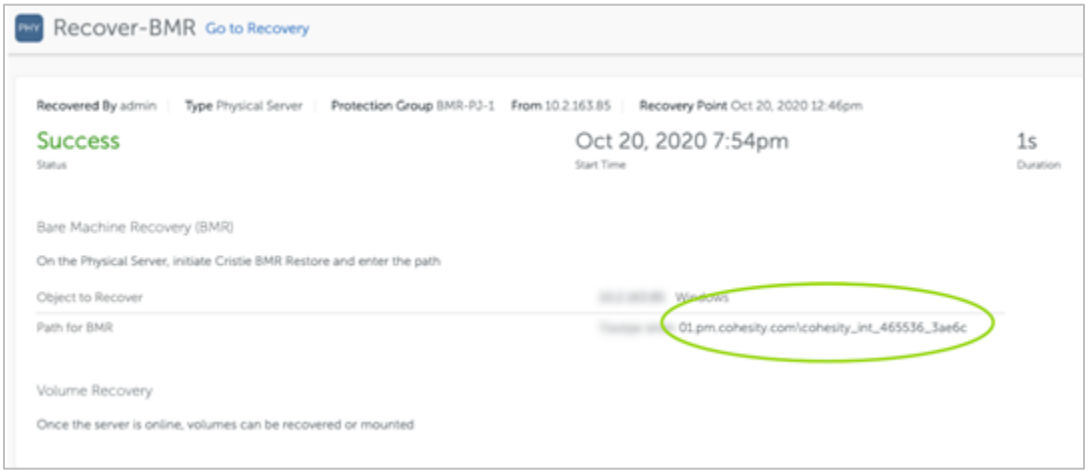
6. Select the **Show only BMR snapshots** option, choose a recovery point, and click **Select Recovery Point**.



7. Accept the auto-generated **Task Name** or enter a new one if you wish to and click **Get Path** to reveal the NFS share path.



8. After a few moments, the **Path for BMR** appears, which is the NFS share path that you will mount in the Cristie recovery wizard. Copy the NFS share path and save it.



> **NOTE**: Make sure to tear down the NFS share after the recovery is complete.

9. On your original or spare Linux machine, mount the NFS path fetched in the previous step.

   Example:

```
mount -t nfs 10.14.17.9:/cohesity_int_670090_f062 /nfs-mount-test
```

> **NOTE**: This validation is an optional step. You can skip ahead to boot the recovery ISO on New Bare Machine.

```
-]#
~]#
~]# mount -t nfs sac01-pm-hoswell6-pl-
vip.pm.cohesity.com:/cohesity_int_670090_f062 /nfs-mount-test
~]#
```

10. Navigate to the mounted path.

    Example:

```
cd /nfs-mount-test
```

```
[root@bmr_linux_sg /]#
[root@bmr_linux_sg /]# cd /nfs-mount-test
[root@bmr_linux_sg nfs-mount-test]# Is
5205389011866424_1604511156205_5082
[root@bmr_linux_sg nfs-mount-test]#
```

11. Change directory into the subfolder and list the directory contents and check if the `system.vtd` file is present.

```
[root@bmr_linux_sg /]# cd /nfs-mount-test
[root@bmr_linux_sg nfs-mount-test]# Is
5Z05389011866Z4_1604511156Z05_508Z
[root@bmr_linux_sg nfs-mount-test]# cd 5Z05389011866Z4_1604511156Z05_508Z
[root@bmr_linux_sg 5Z05389011866Z4_1604511156Z05_508Z]# Is
system.vtd
[root@bmr_linux_sg 5Z05389011866Z4_1604511156Z05_508Z]#
```

You are now ready to boot the recovery ISO.

Boot the Recovery ISO on New Bare Machine

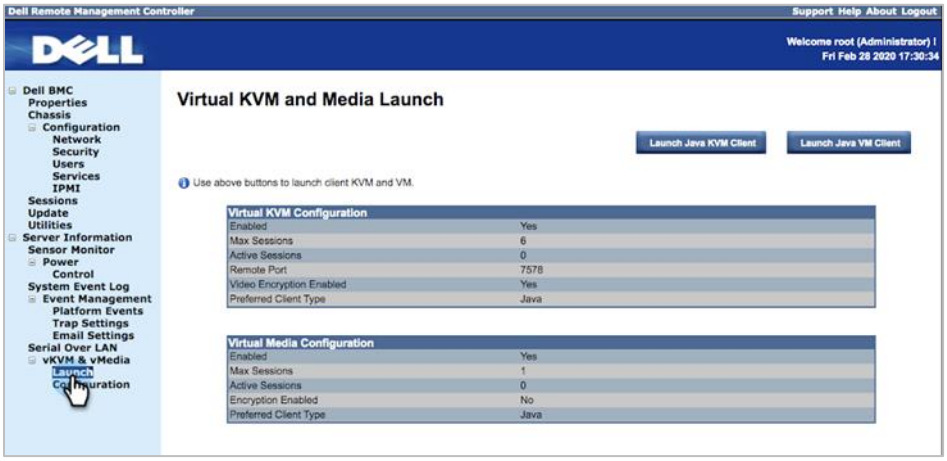
Now that you have the complete path to the ISO image and the system.vtd file, you are ready to boot it on the new bare machine. To do so, you will log in to the IPMI of the bare machine to launch the KVM (keyboard, video, and mouse) console. From there, you will launch the Cristie recovery wizard to recover the protected server onto the new machine.

NOTE:

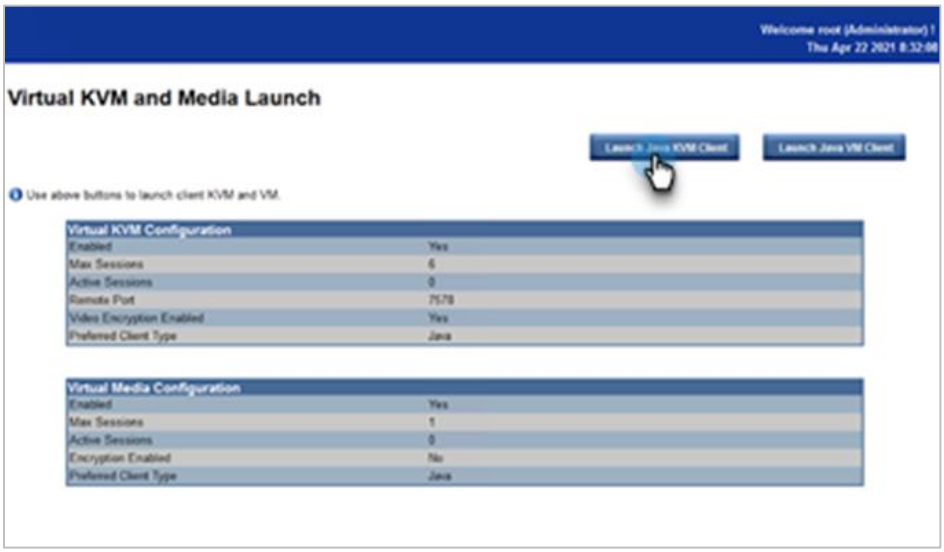
- This process involves recovering your server onto a new bare machine (P2P), but you can also recover it onto a VM (P2V). See Boot the Recovery ISO on a VM.
- In this section, we cover steps to recover to a new bare machine using Dell Remote Management Controller as IPMI. These steps may differ depending on the IPMI you choose.

To boot the ISO on a new bare machine:

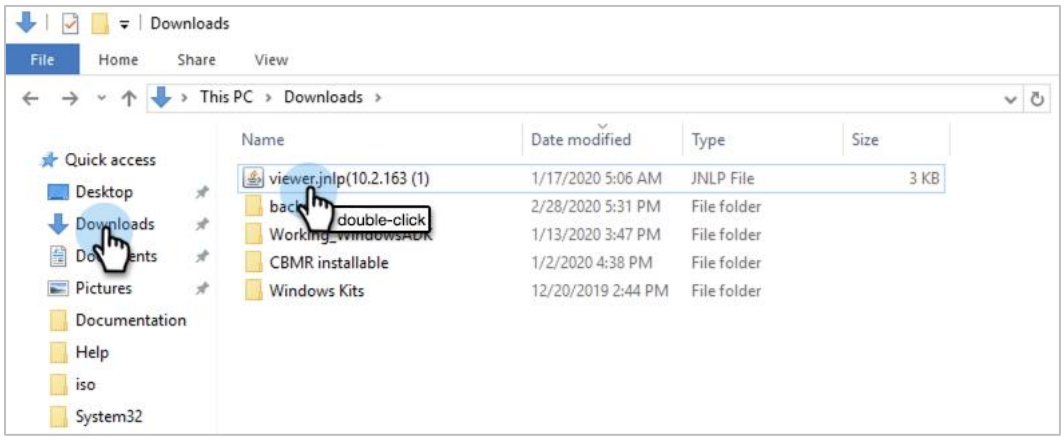
1. Log in to the Remote Management Controller of the new bare machine. Navigate to **Server Information > Serial Over LAN > vKVM & vMedia > Launch**.



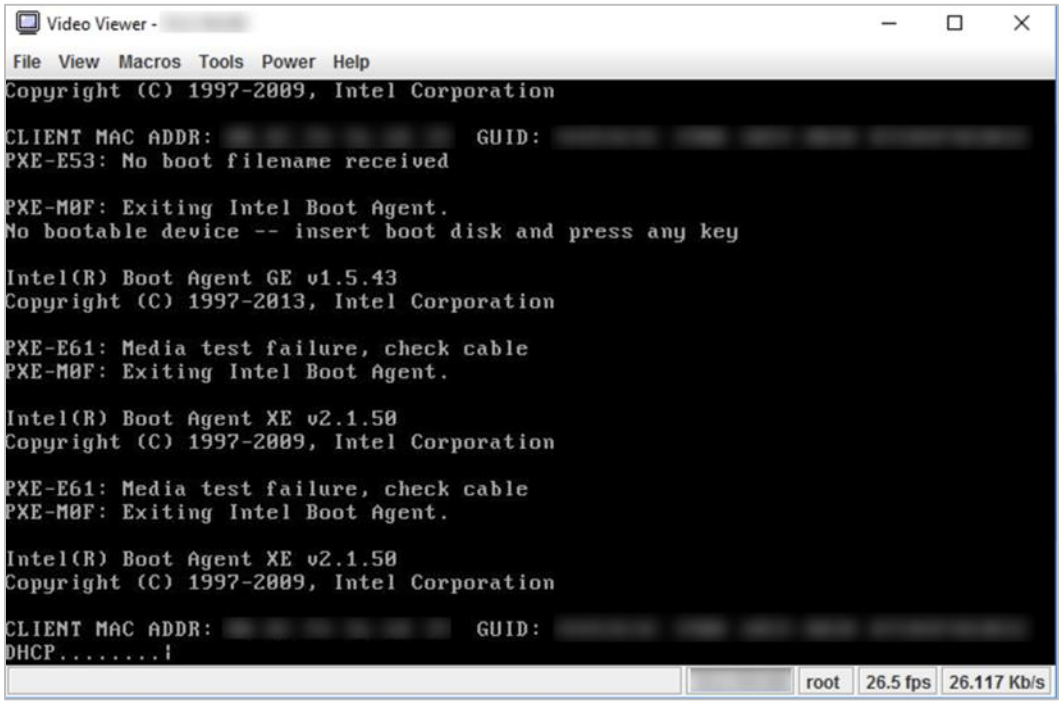
2. Click **Launch Java KVM Client**.



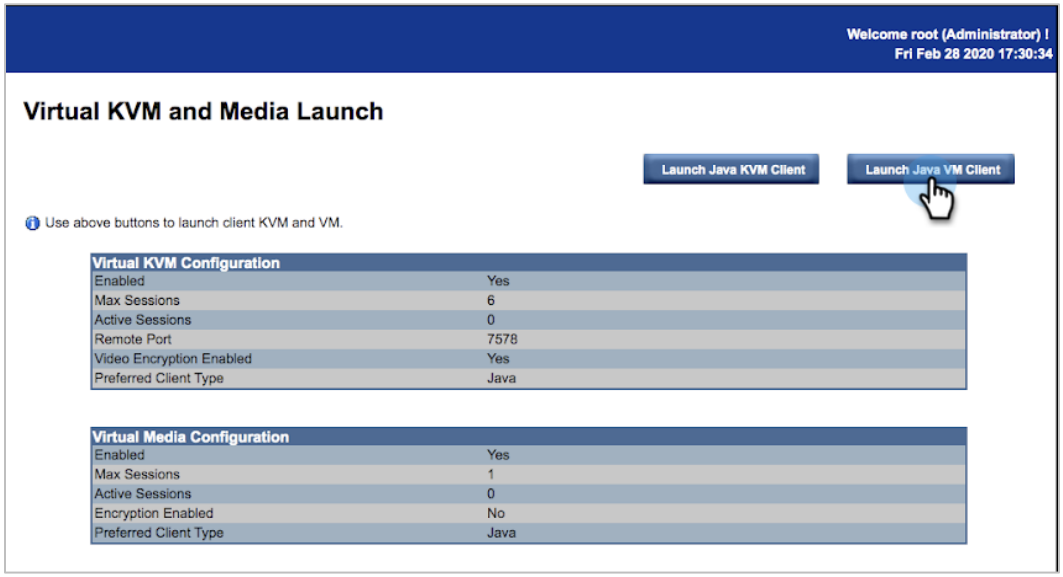
3. Clicking the **Launch Java KVM Client** downloads a Java Network Launching Protocol (JNLP) file, which you can use to launch a KVM session. Launch the `.jnlp` file to start the KVM session.



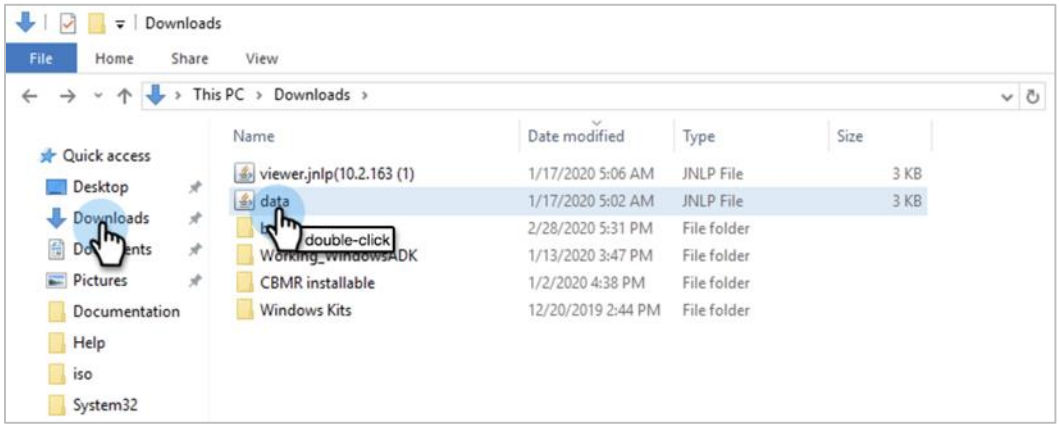
A video viewer running the KVM session opens.



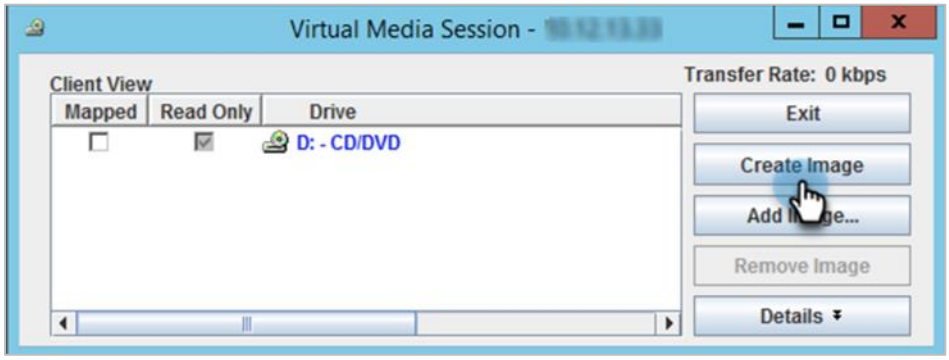
4. Return to the Remote Management Controller and click **Launch Java VM Client**.



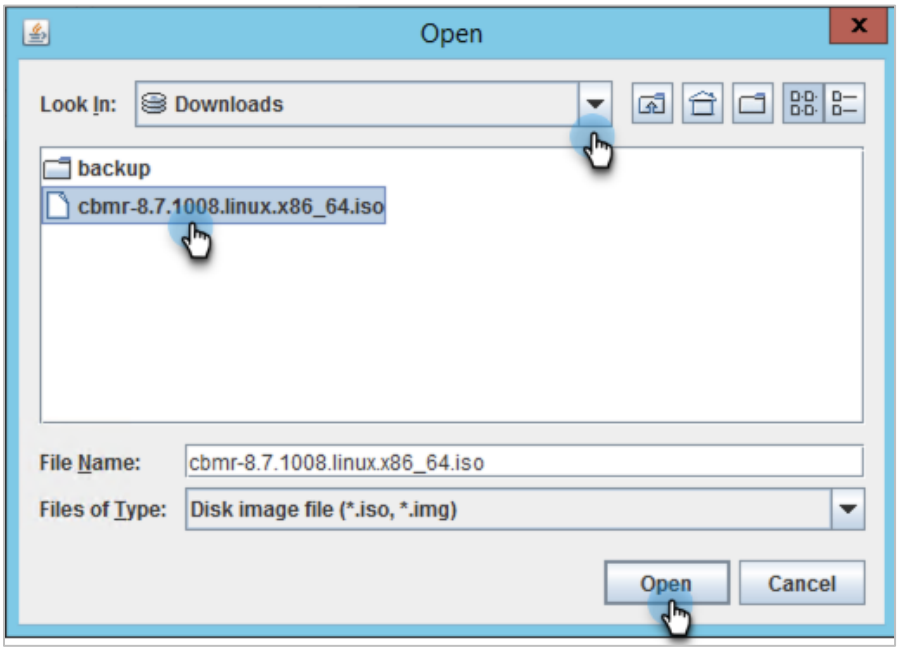
5. Clicking the **Launch Java VM Client** downloads another `.jnlp` file called 'data.' Double-click this file to launch a Virtual Media Session.



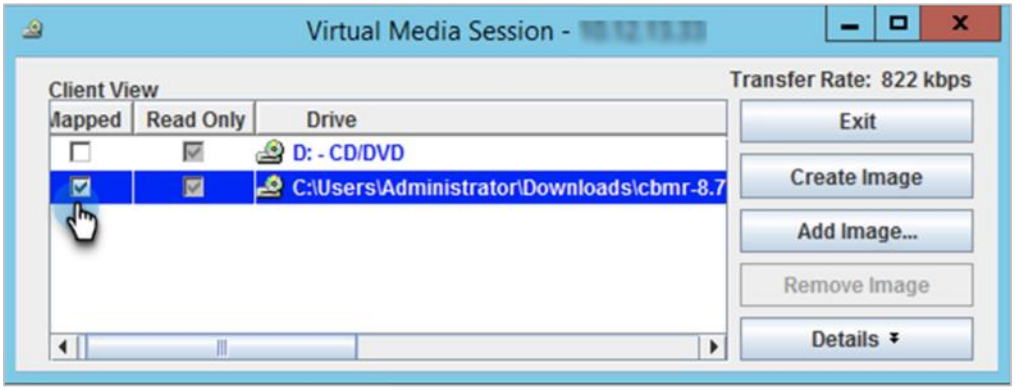
6. A Virtual Media Session opens. Click **Add Image**.



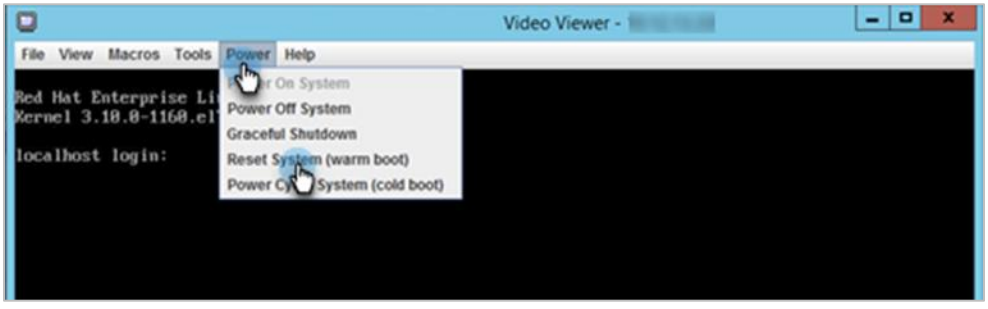
7. Navigate to the folder from where you had downloaded the Recovery ISO image from Cristie. Select the recovery ISO and click **Open**.



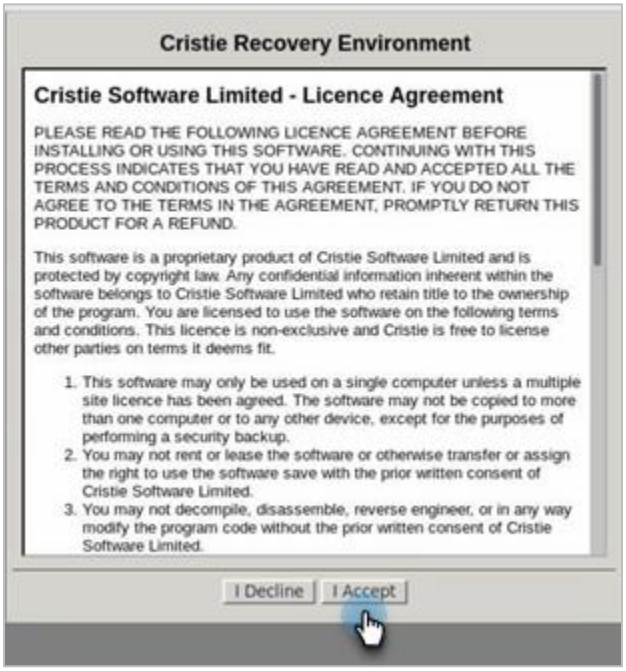
8. Select **Mapped** to map the recovery ISO to the target host.



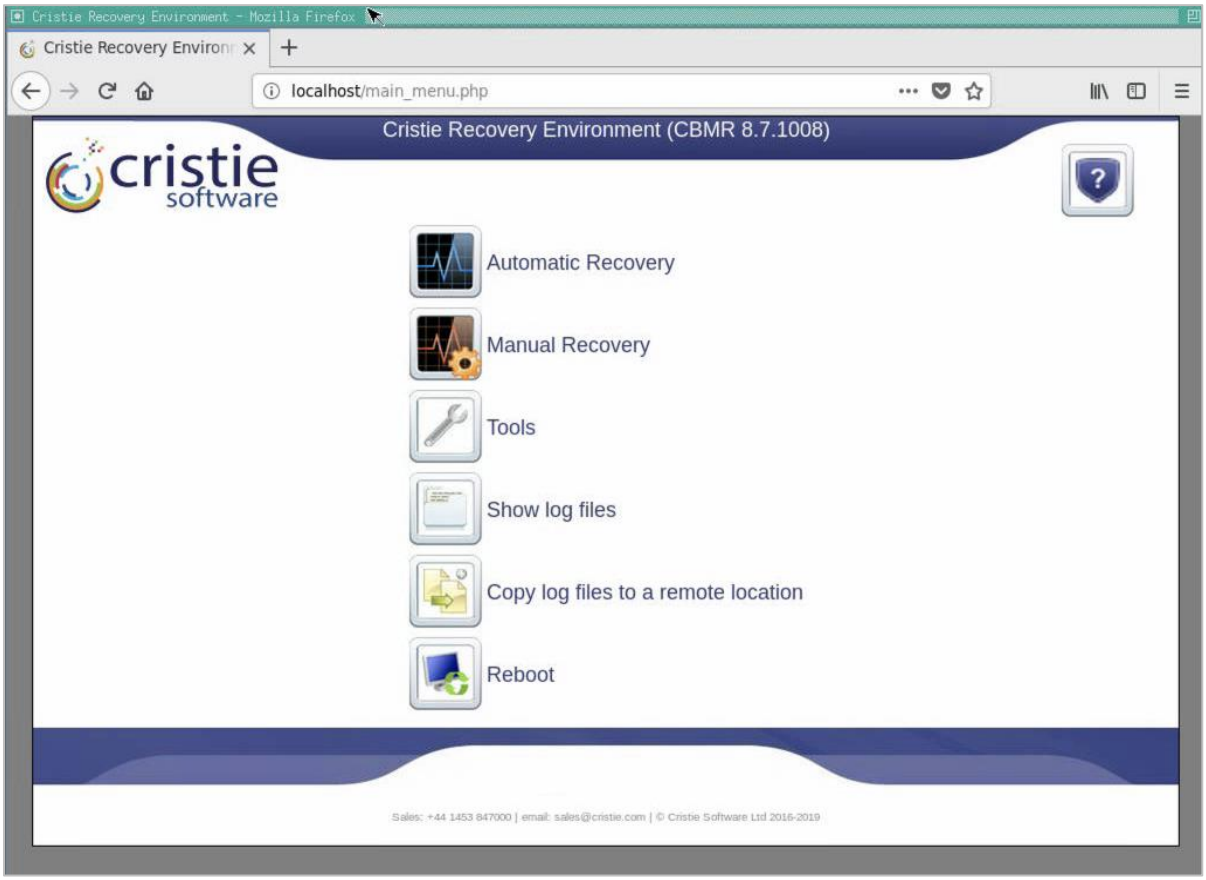
9. Return to the Video Viewer and select **Power** > **Reset System (warm boot)**.



10. On KVM reboot, the KVM session loads the mapped ISO image. **Accept** the License Agreement.



11. Once the License is accepted, the **Cristie Recovery Environment** opens.



To continue, go to Use the CBMR Recovery Environment.

Boot the Recovery ISO on a VM

The recovery process is very similar to restoring a physical server to a virtual machine but takes advantage of VMware vCenter® to load your recovery ISO.

To recover the backup as a VM:

1. Upload the Recovery ISO into the vCenter.
2. Boot the VM using the uploaded ISO.
3. The boot process launches a CBMR recovery wizard. Follow the recovery wizard (in the next section) to complete the recovery.

For detailed instructions on deploying a VM from an ISO, see Deploy a Virtual Machine from a Template in VMware's documentation.

To continue, go to Use the CBMR Recovery Environment.

Use the CBMR Recovery Environment

When the recovery ISO is booted, it initiates an OS installation-like boot procedure. The boot process loads the Linux driver, and the CBMR Recovery Environment opens.

To recover a server to its original state using the CBMR automatic recovery wizard:

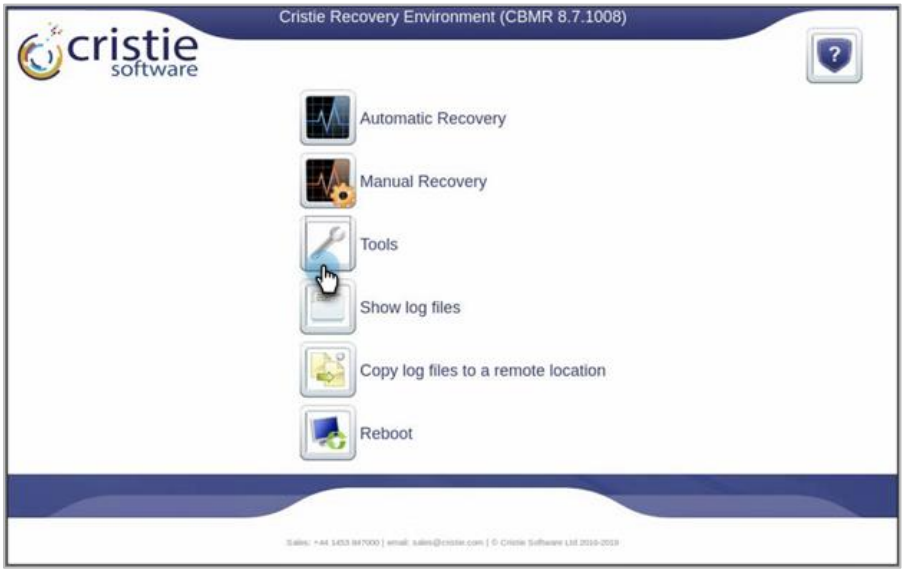
1. Configure the network to access the NFS share exposed from Cohesity.
2. Use the recovery wizard to initiate recovery.

Configure the Network

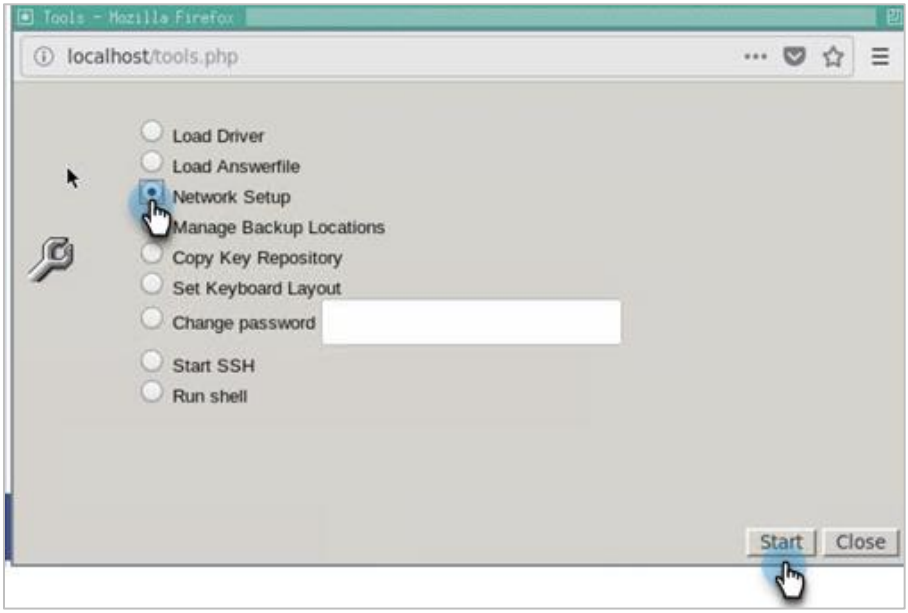
The server marked for recovery must be configured in the network to access the NFS share from Cohesity. We recommend that you configure the network before you initiate the automated recovery.

To configure the network for recovery:

1. From the CBMR wizard, click **Tools**.



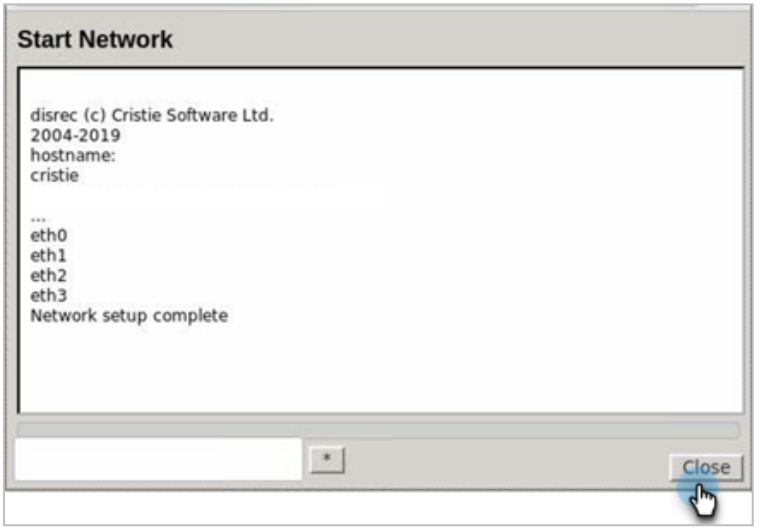
2. From the **Tools** window, select **Network Setup** and click **Start**.



3. In the **Network Setup**, configure the network to an IP address and gateway. You have two configuration options:
   - **Enable DHCP** to Obtain an **IPv4 address automatically** for dynamic IP address allocation.
   - For **Static IP configuration**, enter a valid **IPv4 Address**, **Subnet Mask**, and **Gateway**.
   - Click **OK**.

NOTE: Make sure the IP address is accessible from Cohesity.

4. Once the network setup is complete, click **Close**.

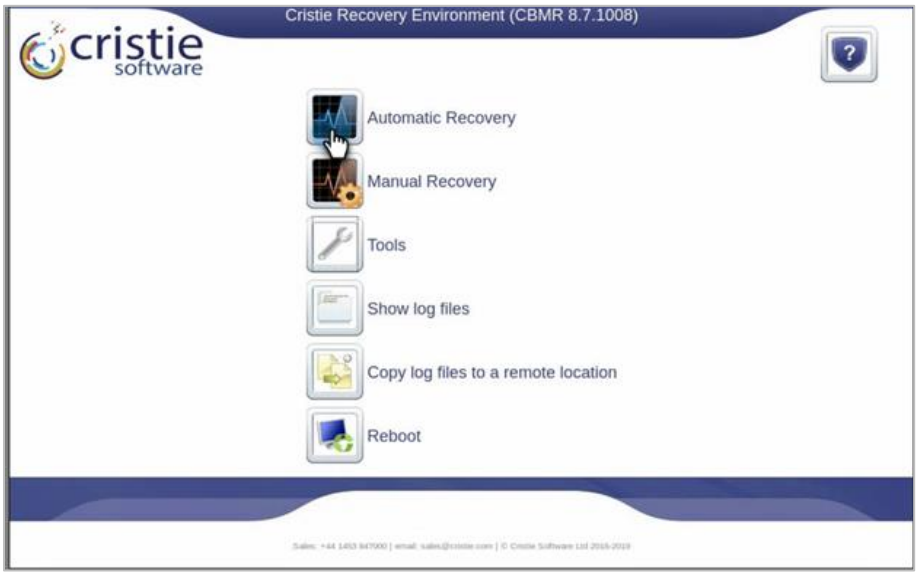


Use Recovery Wizard to Initiate Recovery

With CBMR Automatic recovery wizard, a restore sequence automates access configurations and file restores. You will have the option to choose the hostname and the network settings of the target machine. The target hardware may be different from the source hardware. In such cases, you can load the additional drivers required for the new hardware.

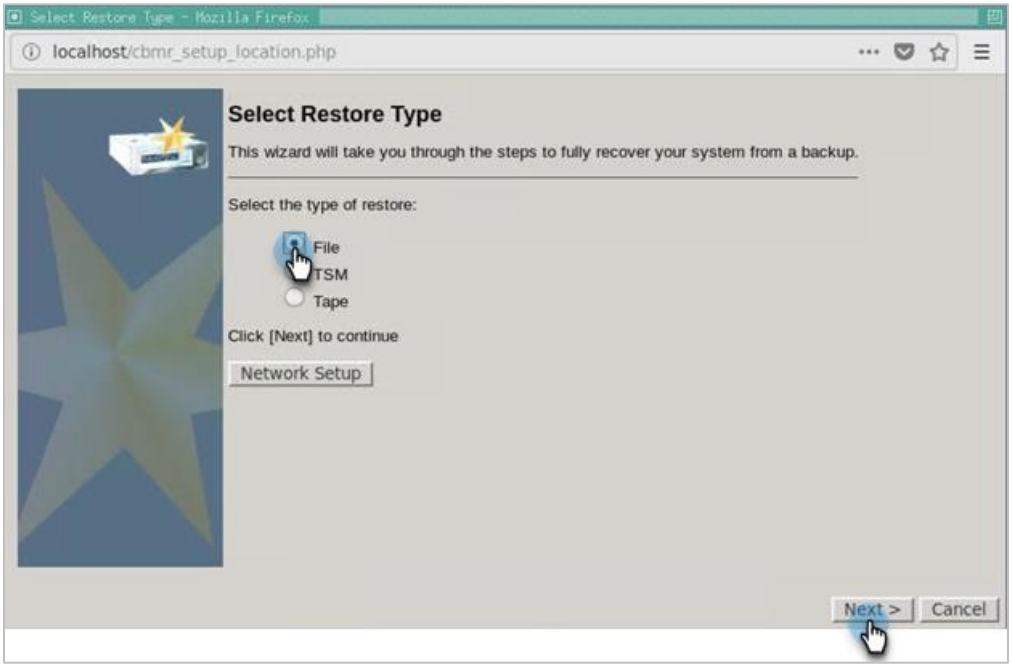
To initiate recovery:

1. In the CBMR wizard, click **Automatic Recovery**.



NOTE: Automatic Recovery workflow handles the recovery process and configurations. However, you can select Manual Recovery if you wish to have greater control in restoring your systems (for example, in creating and formatting partitions and volumes).

2. Select **File** as the restore type and click **Next**.



3. On the following page, the wizard prompts you to enter the location to the Virtual Tape Drive (.vtd) file. Click **Browse** and select **Mount Network Share / Device**.

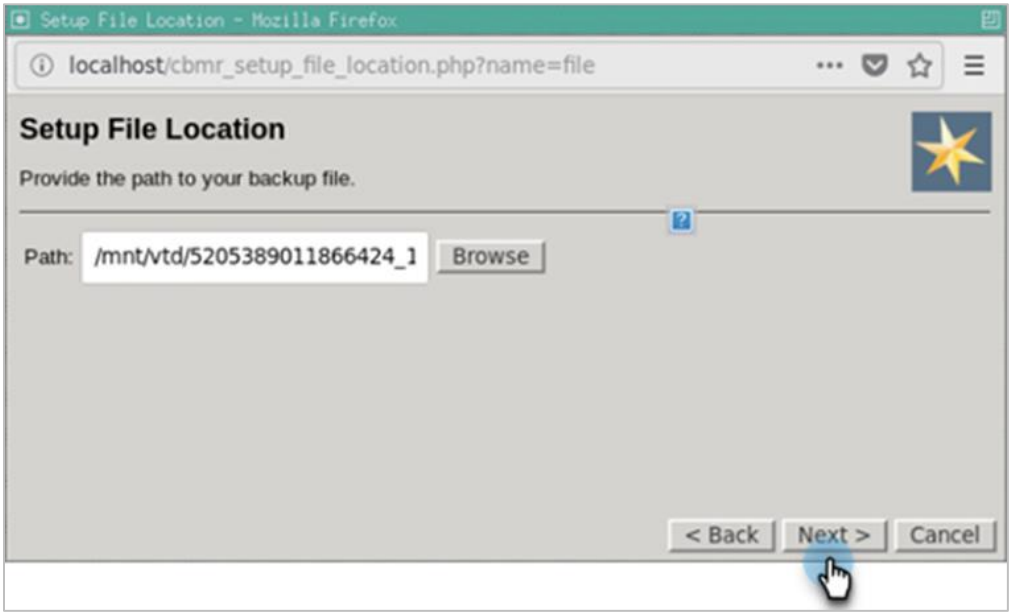
4. In the **Mount Network Share/Device** screen, enter the following details:

   a. **Share / Device**: The recovery path fetched from Cohesity.
   b. **IP Address**: Enter the FQDN / IP address of your Cohesity environment
   c. **Domain**: Enter the domain details of your Cohesity environment

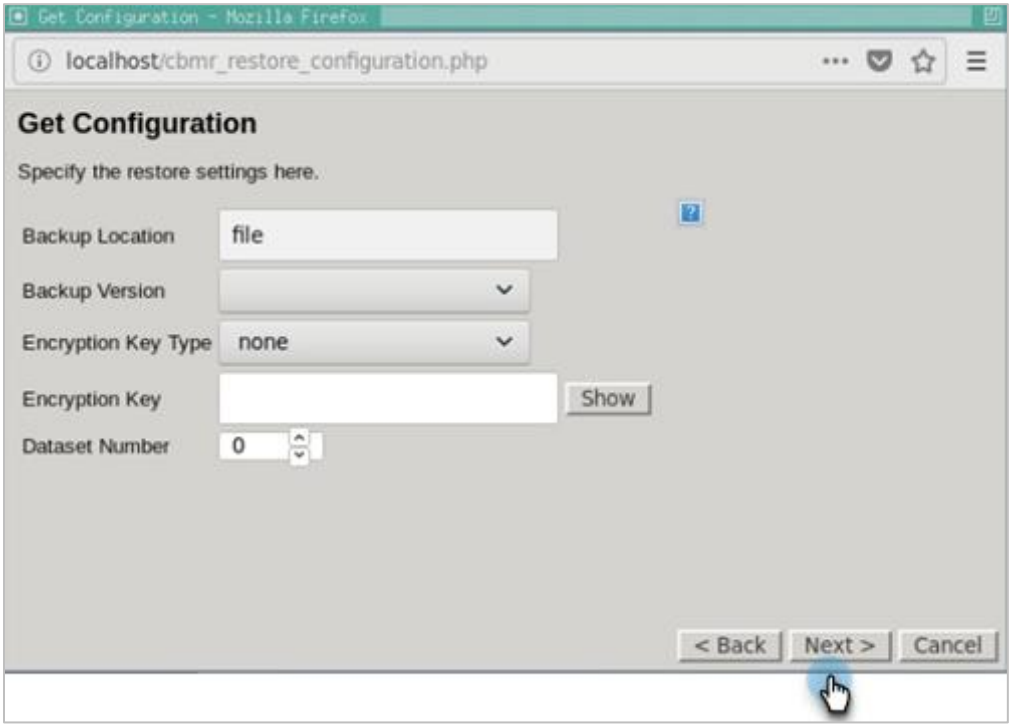
   Click **OK** to mount the NFS share.

5. CBMR Recovery Environment mounts the NFS share. Click **Close**. Then click the mounted drive and select the `system.vtd` file.

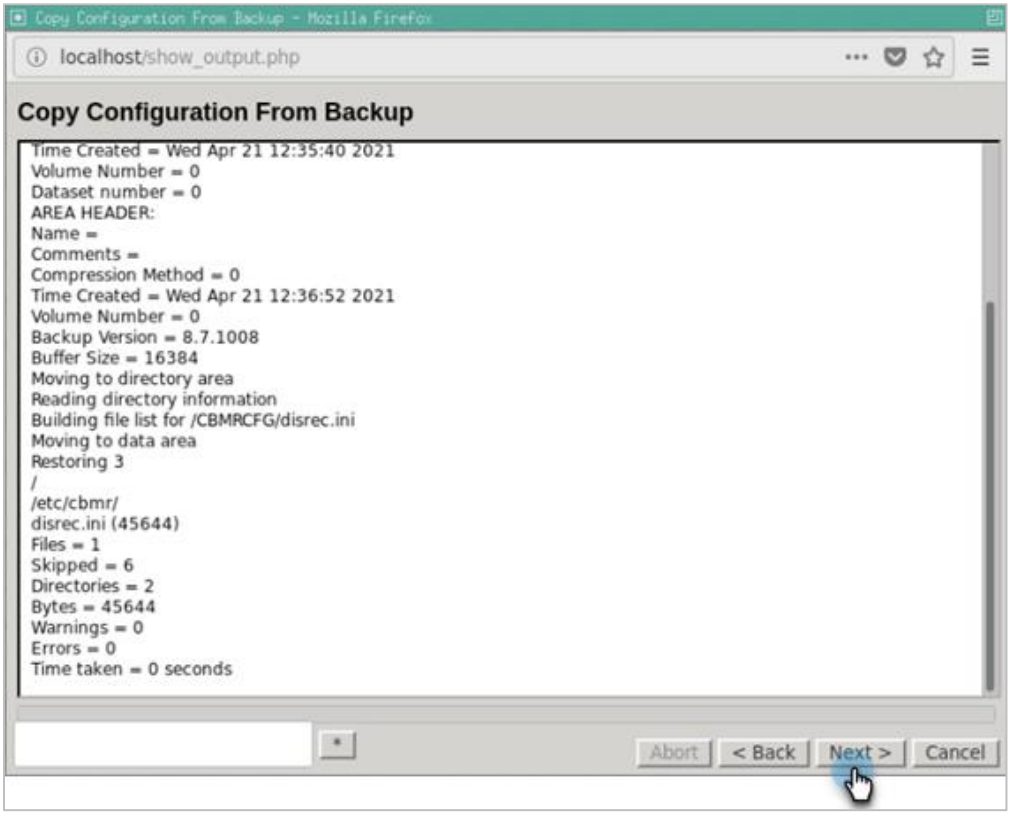
6. Click **Next** to continue.



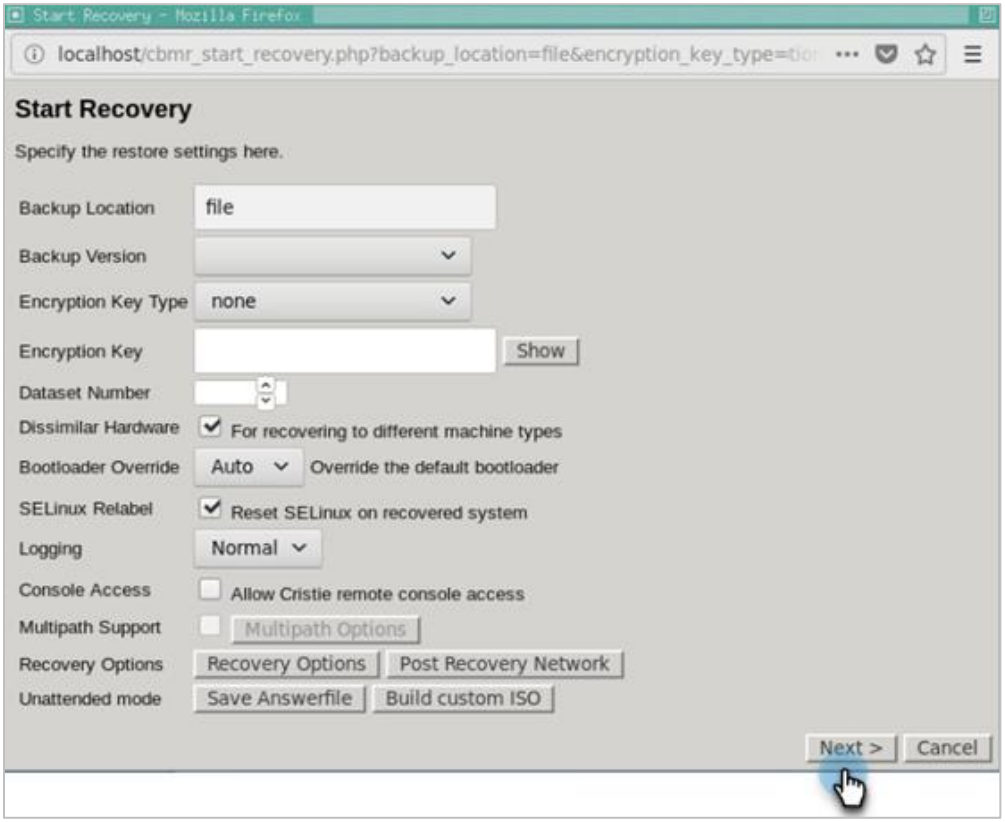
7. Specify the Configurations (if any) and click **Next**.



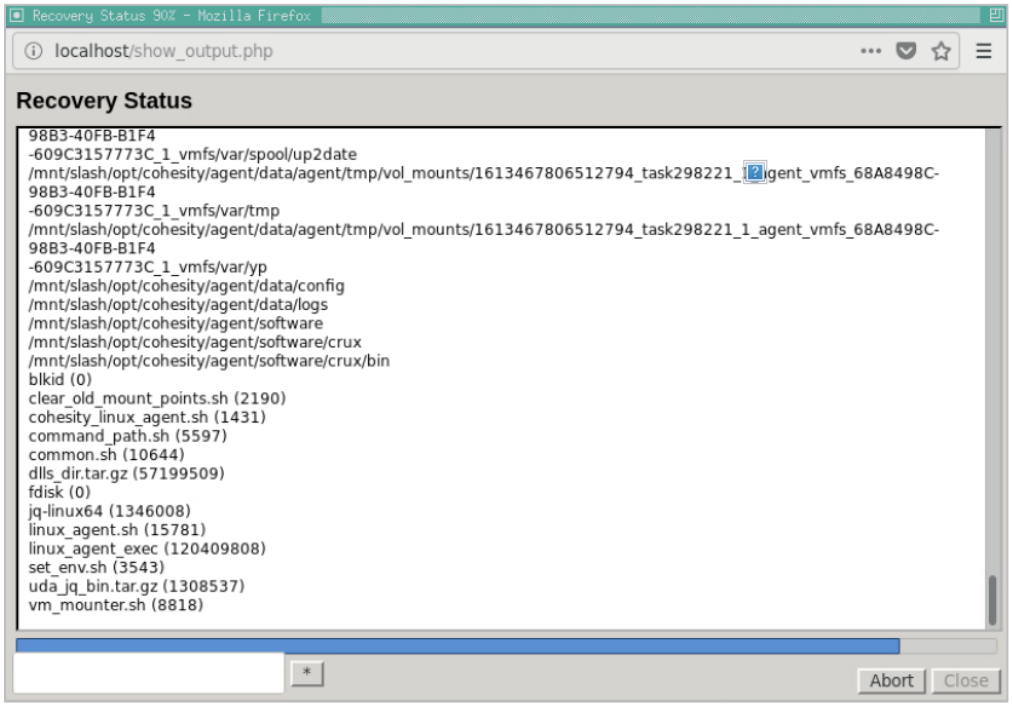
8. Click **Next**.



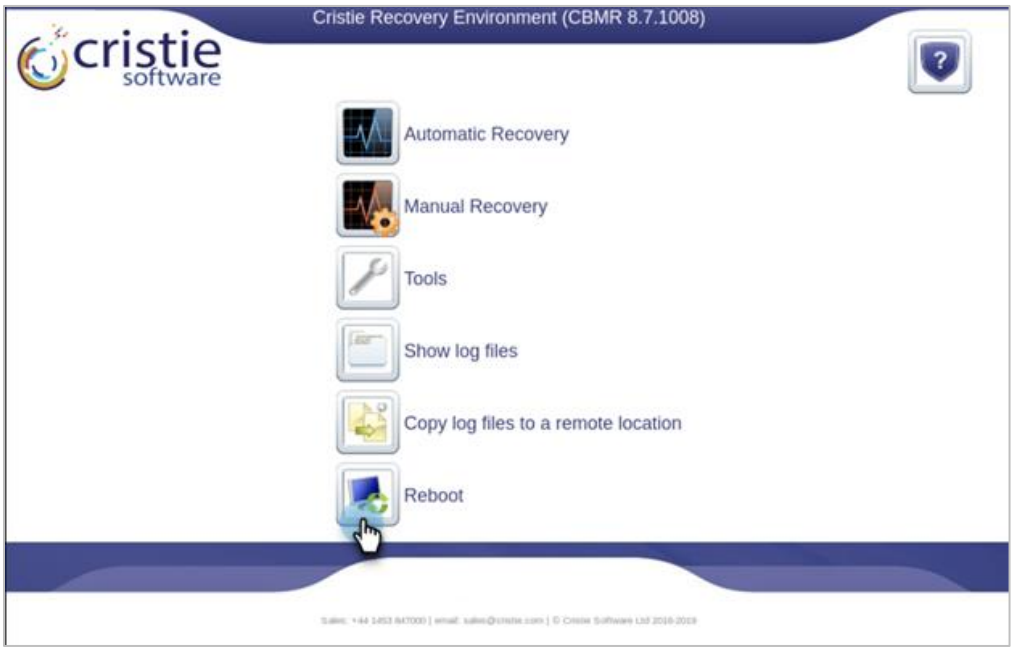
9. Review the restore settings and click **Next** to start the recovery.



10. The CBMR recovery process transfers the data backed up on Cohesity and restores them on the target server to create a replica of the original server. The **Recovery Status** dialog displays the progress through the recovery process.



11. CBMR recovery wizard completes the recovery by restoring all the mounted filesystems from the source. Click **Reboot** to complete the recovery.



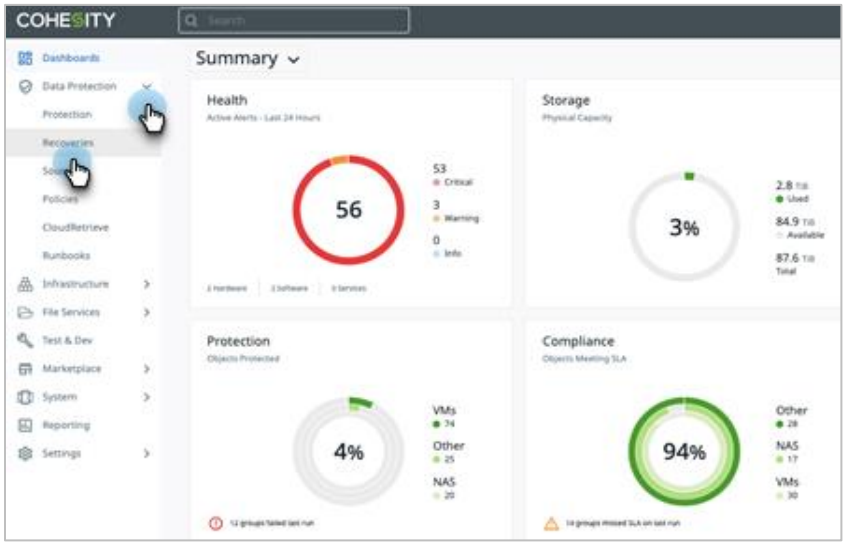
12. Log in to the target machine and validate the recovery.

Tear down the NFS Share

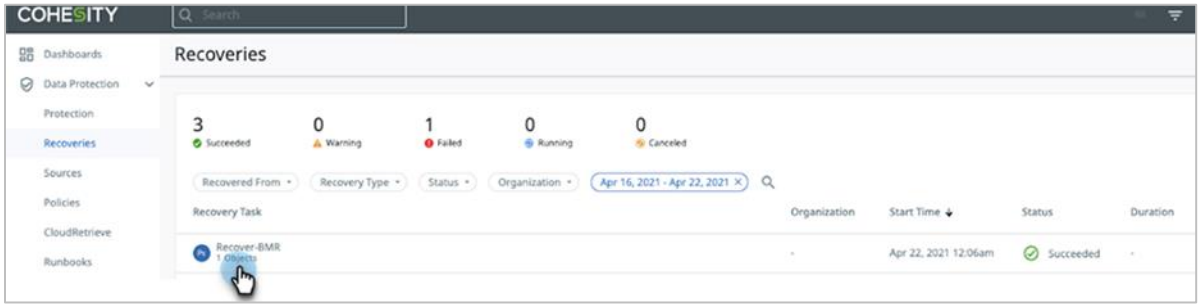
The recovery workflow initiated from Cohesity opens a gateway to fetch the Virtual Tape Drive (.vtd) file. Leaving this connection open is a security risk. As a best practice, we recommend you tear down the exposed NFS path after completing the recovery.

To tear down the NFS share:

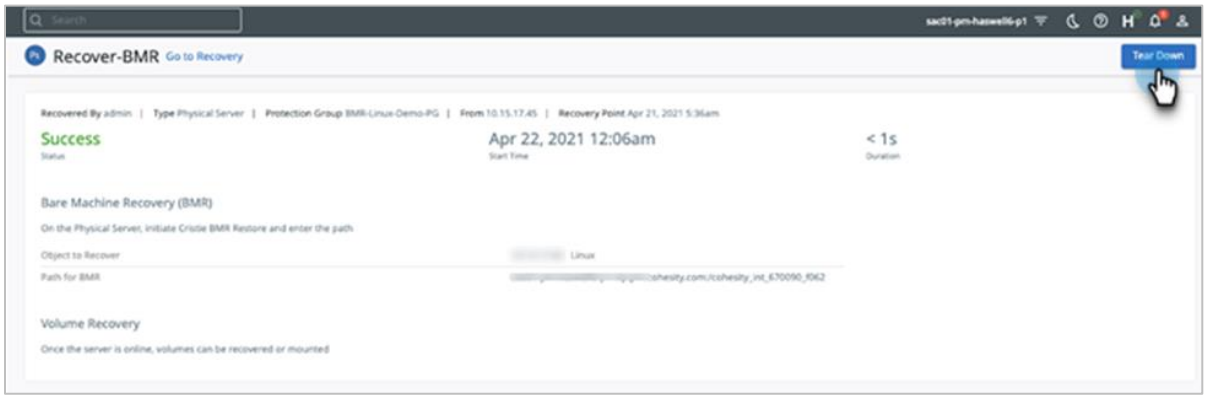
1. Log in to Cohesity.
2. Navigate to **Data Protection > Recoveries**.



3. Select the recovery task used for fetching the NFS



4. Click the **Tear Down** button from the top right corner to delete the recovery path.



You have now recovered and restored your server onto a bare machine.

Appendix A: Troubleshoot BMR

For information about troubleshooting BMR, see How to troubleshoot Cristie Bare Machine Recovery (Cristie BMR) in the Cohesity Support portal.

Appendix B: Cristie Resources

Use these links to register your Cristie software, activate your license, and read the Cristie documentation:

- Cristie Registration
- Licensing Portal
- CBMR documentation
- CBMR User Guide
- CBMR Installation Guide
- CBMR support matrix

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Surya Swaminathan is a Sr. Technical Marketing Engineer at Cohesity. In his role, Surya focuses on the cloud, manageability, and disaster recovery.

Other essential contributors include:

- Arvind Jagannath, Product Management
- Adaikkappan Arumugam, Sr. Manager Technical Marketing & Solution Engineering
- Bart Abicht, Senior Technology Writer and Editor at Cohesity
- Gautam Bhasin, Product Management
- Subash Babu, Staff Technology Writer and Editor at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	July 2021	First release

ABOUT COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

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