COHESITY

Version 1.2

Dec 2020

Bare Machine Recovery Using Cohesity & Cristie

Use Cristie BMR with Cohesity for Bare Machine Recovery

ABSTRACT

Physical Server backup and recovery entails challenges because servers contain not only user directories but also system directories that need to be restored 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 for subsequent recovery, either into the same server or an entirely new server. Cohesity ensures continuous protection of the server, and any point in time recovery.

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 a challenge because the vendor landscape has many players with varying capabilities and support structures, and 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 the user does 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 servers runningthe Microsoft Windows® OS with the Cohesity Agent for Windows installed.

Cohesity has partnered with Cristie Software, a company established in BMR, to provide a comprehensive backup & recovery solution for servers. Achieving your recovery objectives is now simpler with Cohesity™. While Cristie Software's Bare Machine Recovery (CBMR™) software enables you to extract and bundle your system data files, Cohesity works with CBMR to back up both user volumes and system data. This helps backup administrators easily back up and restore Windows, including user volumes and system data, 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 servers using Cristie BMR 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 platform that is simple to manage. For BMR, Cohesity integration with Cristie BMR facilitates automatic backups and accelerated recovery of servers directly from backups.

Cohesity's partnership with Cristie BMR enables enterprises to:

- **Restore Servers Quickly**. Boot from a preconfigured Windows Preinstallation Environment (WinPE) ISO image to start the recovery process. This 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. Use Cohesity's advanced algorithms for compression and deduplication to dramatically reduce storage consumption and lower the cost of protection.
- **Secure Data**. Cohesity employs both in-flight and at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) encryption standard.

Terminology

There are several concepts and terms that are important to understand as you learn about Cohesity's data protection solution for servers.

Table 1: Terminology for BMR with Cohesity

TERM	DEFINITION
Cristie BMR	The Cristie Bare Machine Recovery software that enables server recovery onto a bare machine.
CRISP	The Cristie Recovery ISO Producer. This can be used to produce a recovery ISO that is customized to recover system files that are bundled into a single Custom Virtual Device Driver file (.VTD File).
WADK	Windows Assessment and Deployment Kit for Windows provides deployment tools for automating large-scale deployments of Windows Servers.
Windows PE	Windows Preinstallation Environment (WinPE) is a minimal Windows operating system that provides limited services based on the Windows kernel. Required to run Windows Setup, access and install operating systems from the network, script basic repetitive tasks, and validate hardware.

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, you install Cristie BMR (CBMR) on the server you need to protect to back up the server's boot drive. On the same server, you will install the Cohesity Agent for Windows, which facilitates communication between CBMR and Cohesity. This allows you to back up the entire server using a single Cohesity Protection Policy.

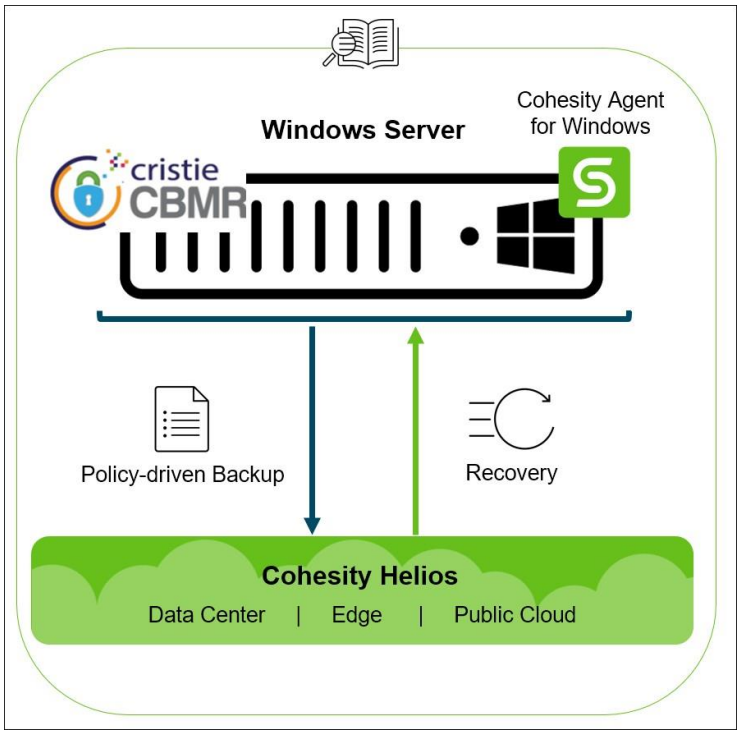
When you set up protection for your server, you create two schedules: one for backing up the volume data and another, less frequent schedule for backing up your boot drive.

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. This is achieved by the Change Block Tracking filter driver that is installed as part of the Cohesity Agent for Windows, which runs as a lightweight service.

NOTE: Until the first reboot after the Cohesity Agent for Windows is installed, it will continue to performfull instead of incremental backups. After reboot, the filter driver will be able to capture just the changeddata in incremental backups.

When Cohesity triggers CBMR to back up your machine configuration, it runs a full backup each time. The CBMR backup protects everything on the server's boot drive.

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 systems can be restored from a potential failure. The magnitude of failures 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.
- Colossal damage to the hardware.
- Data center outage due to natural calamity.
- Migrating to an environment running on dissimilar hardware.

A bare machine recovery is suitable in scenarios where there is a need to rebuild your infrastructure efficiently. With Cohesity and Cristie BMR integration, you can take advantage of the Cohesity agent for Windows and CRISP (the Cristie Recovery ISO Producer) for a tried-and-tested disaster recovery solution. By creating a Custom Virtual Device Driver (.vtd) file with all the volume and system data, and by creating a bootable environment, the entire recovery process is made simple, reliable, and fast.

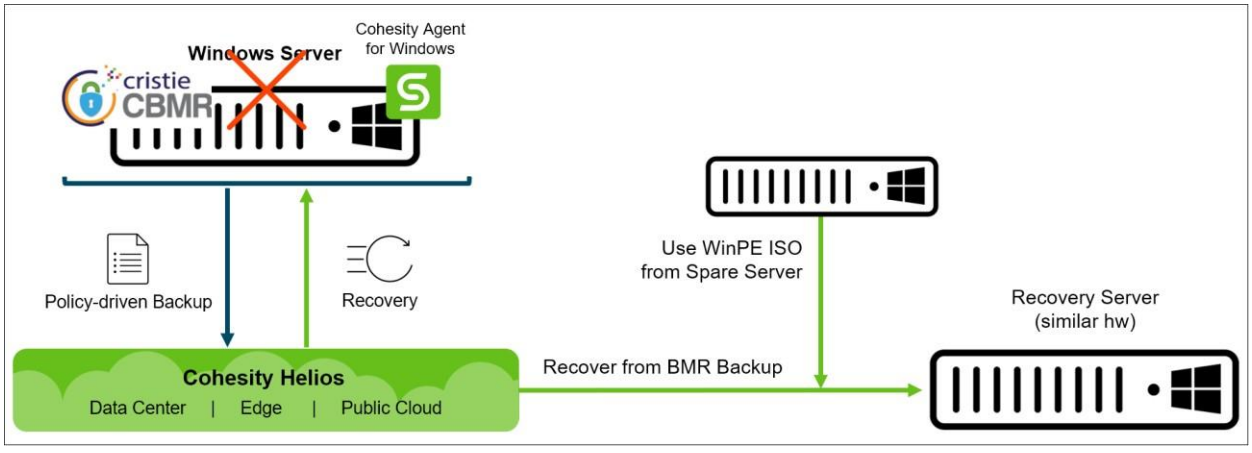
To mitigate data loss, we need to be prepared in the event of a failure. Below, we discuss three such recovery scenarios.

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)

If a malware attack deletes all the data on your server but the server is still accessible, you can recover the system back to a stable state on the original machine.

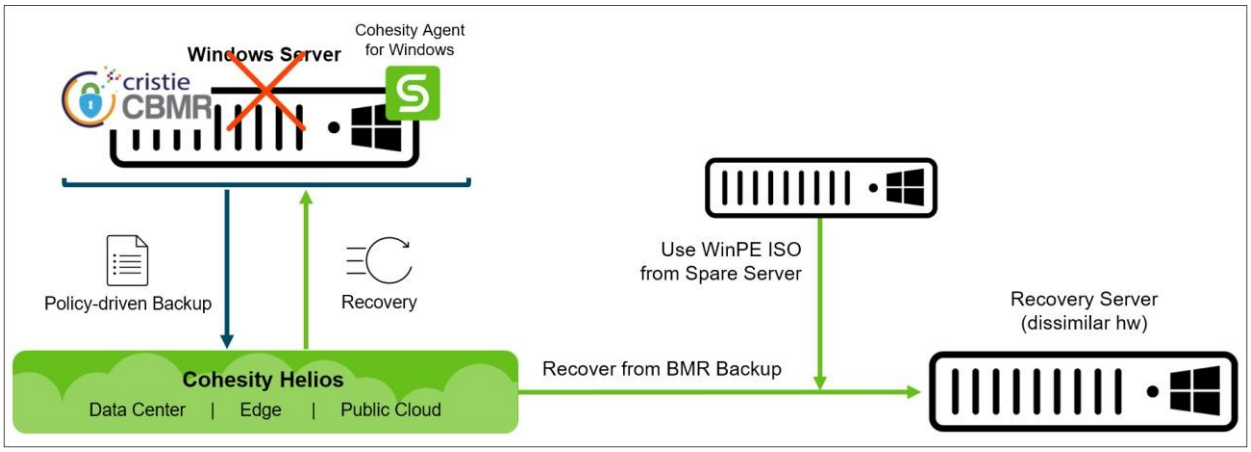
Figure 2: P2P Workflow—Recover Server to Original Machine



Recover Server to New Machine (P2P)

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

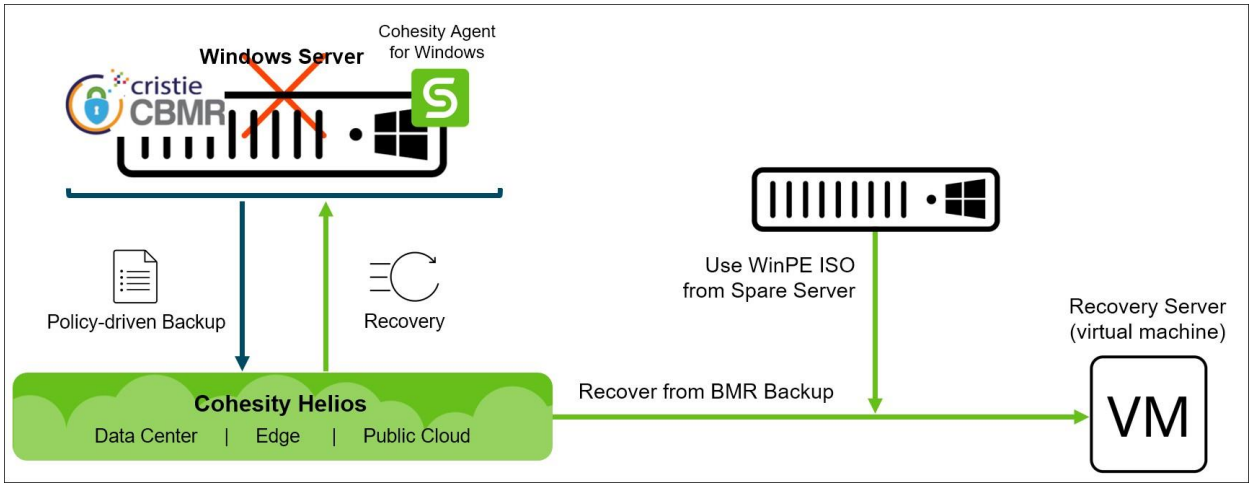
Figure 3: P2P Workflow—Recover Server to New Machine



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 useful 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 using CBMR and recover your protected VM. However, VMWare's native recovery method is more effective in this scenario.

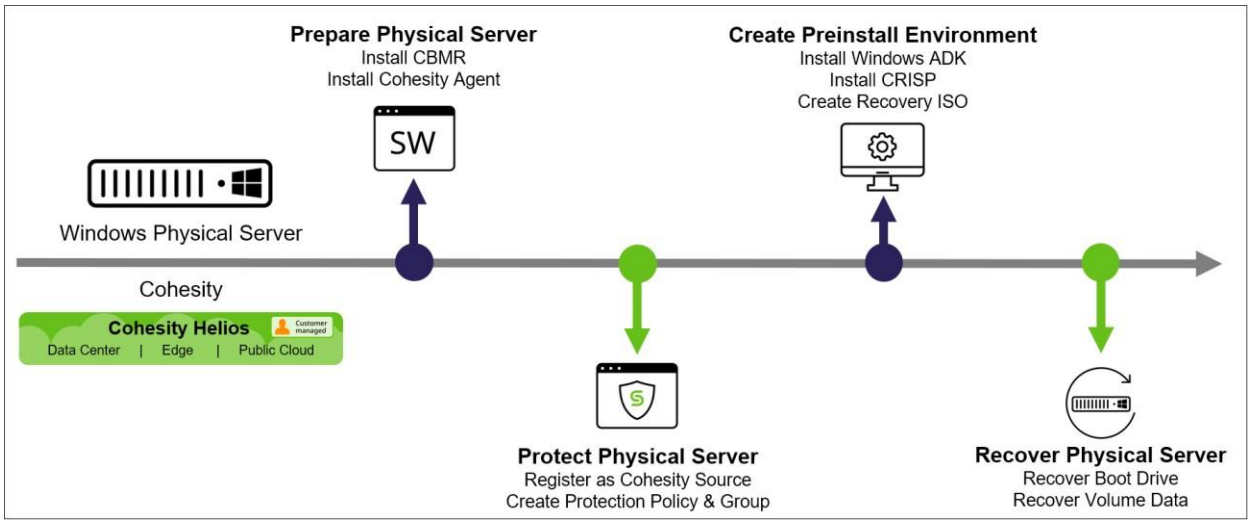
Set Up BMR with Cohesity

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

To set up and start using CBMR with Cohesity, there are several tasks to perform:

1. Prepare the server for Cristie-Cohesity integration.
2. Register your server as a Cohesity source and set up protection.
3. Create a preinstallation environment and boot ISO.
4. Recover your server using Cohesity and CBMR.

Figure 5: Cohesity with Cristie BMR Solution Workflow



Prepare the Server for Cristie-Cohesity Integration

CBMR (Cristie BMR) 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 Windows 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 Windows on the same server.

Install Cristie BMR

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

- A server running a supported Windows OS. See **Physical Servers** in the Supported Software list for Cohesity-qualified versions.
- Login credentials for the Administrator user on the server.
- A licensed version of the qualified Cristie BMR Suite. See **Cristie BMR** in the Supported Software list for Cohesity-qualified versions.

To install CBMR:

1. Download your licensed Cristie BMR installation binary and run it. Follow the prompts to select your language, accept the License Agreement, and select **Install CBMR Suite**.
2. In the Select install component dialog that appears, select **Install CBMR**.

3. Select a location and click **Install**.
4. When the process completes, click **Finish** and reboot the server.

IMPORTANT: Remember to register with Cristie and activate your Cristie license within the fully functional

Install the Cohesity Agent for Windows

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

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

Protect Your Windows Server

Protecting your Windows server with Cohesity and CBMR involves two Protection schedules, one with frequent Protection Runs for the data and another for less frequent Protection Runs to save your machine's configuration to prepare for the eventual need to restore the server (onto the original or dissimilar hardware).

Once you register your Windows 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 enables the Cohesity agent for Windows to work in conjunction with CBMR to ensure continuous protection of the servers.

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. This helps you avoid having to re-register 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

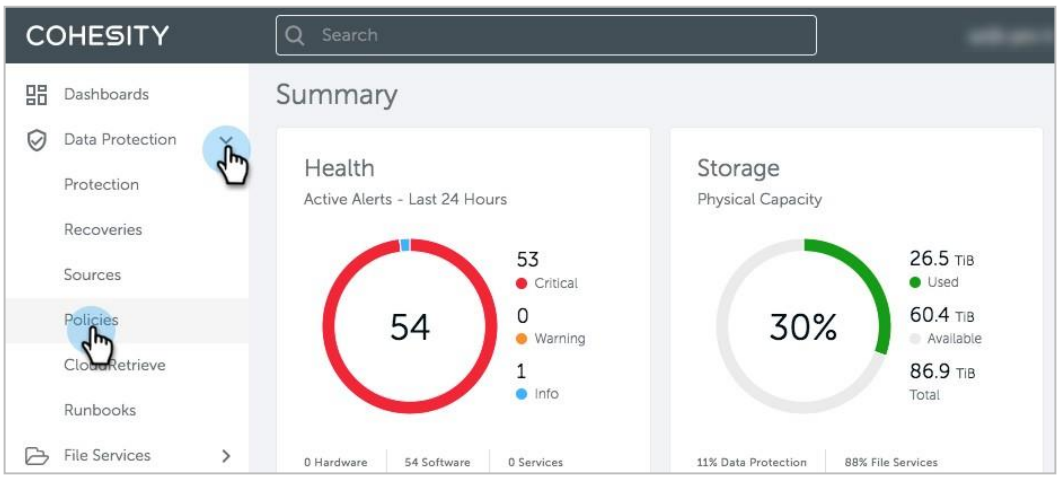
In Cohesity, Protection Groups use Protection Policies. Protection Policies reflect business needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), while a Protection Group defines operational requirements, 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:

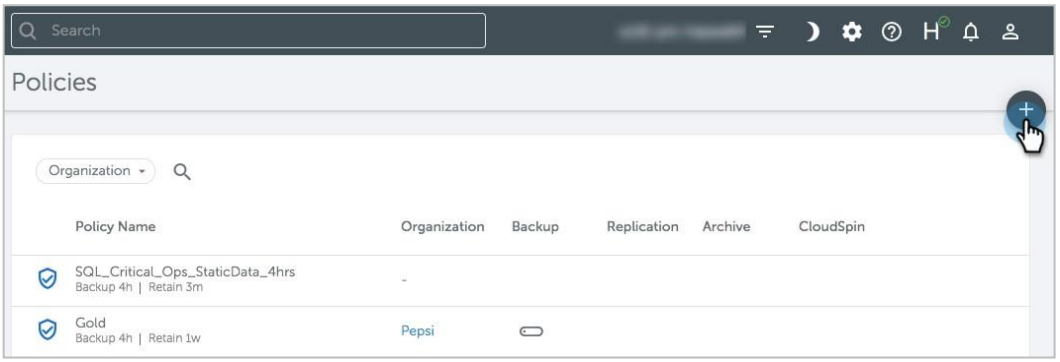
- How source data (like virtual & physical servers) is protected (backup, replication, and/or archival).
- The frequency of Protection Runs.
- Where the data is stored.
- How long the backed up data is retained.

To create a BMR-enabled Protection Policy:

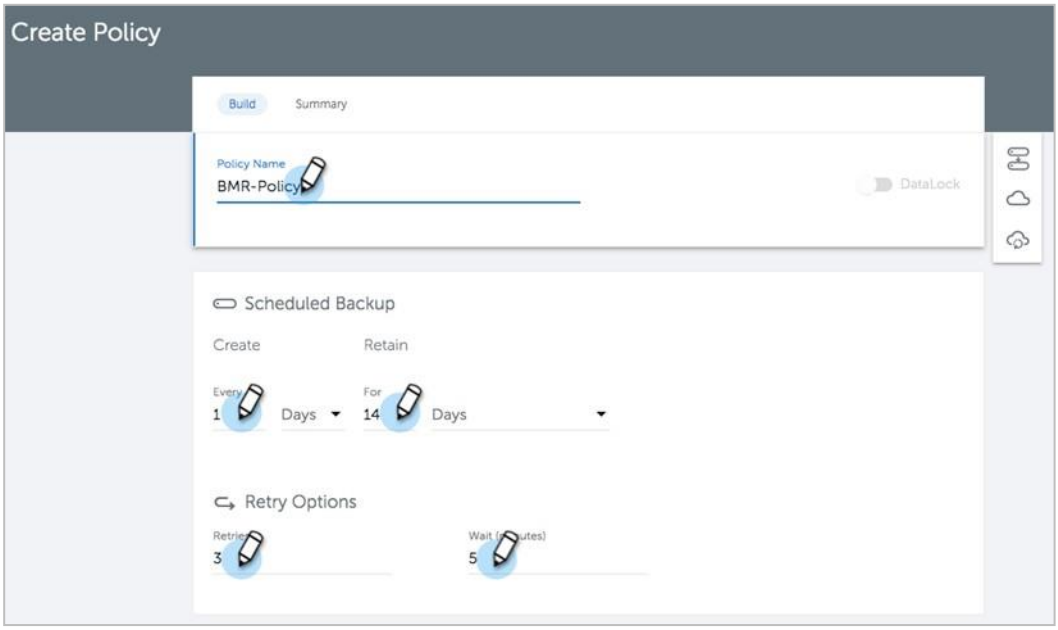
1. Log in to Cohesity.
2. Navigate to **Data Protection** > **Policies**.



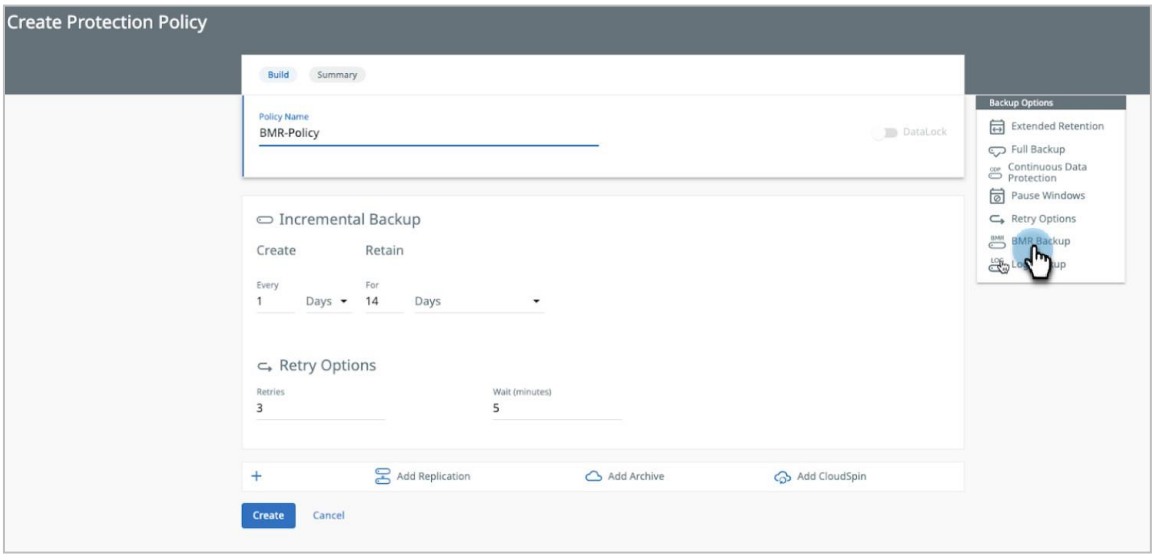
3. Click the **Add** button.



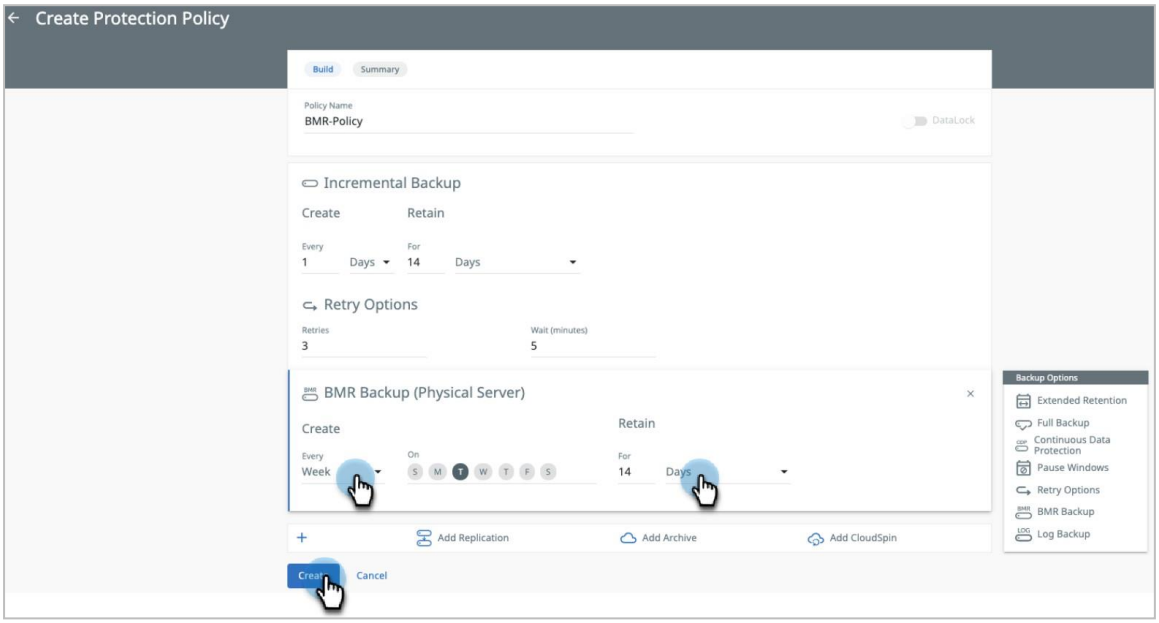
4. In the **Create Policy** form, enter a **Policy Name**, select the interval and retention times for the **Scheduled Backup** for the data (volumes) on your server, and edit the **Retry Options** if necessary.



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 if necessary. Then click **Create**.



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

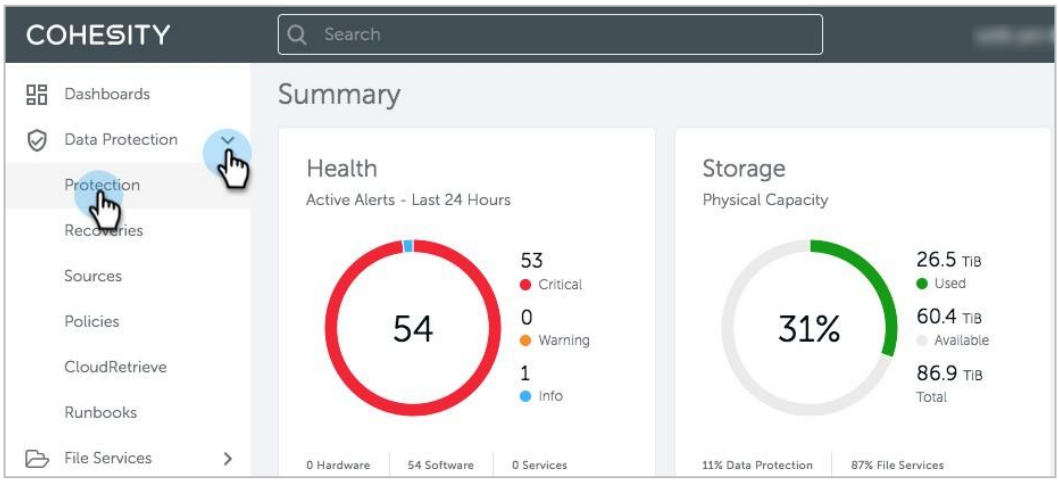
Create a Protection Group

Protection Groups combine operational requirements with the business requirements that are 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).

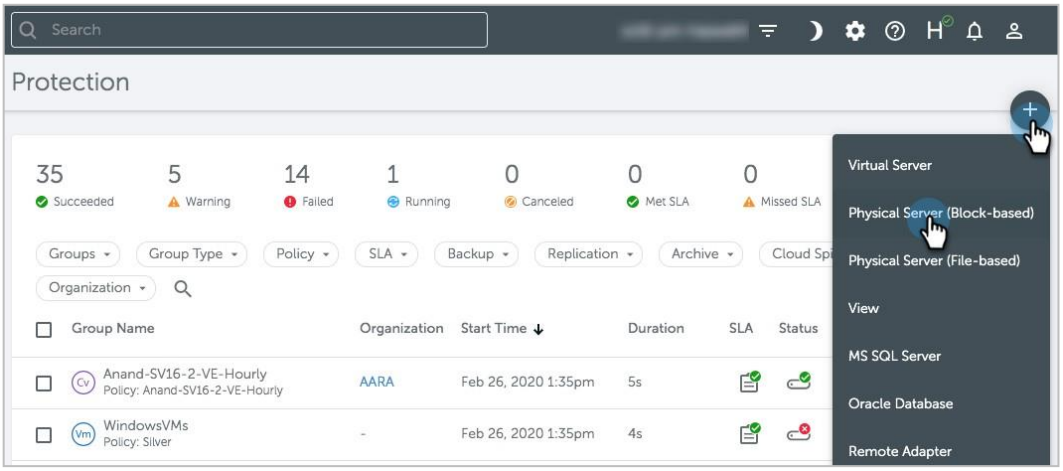
The process to create a BMR specific Protection Group is very similar to steps involved in protecting other sources except for an additional step to enable BMR backups. The steps to enable BMR backups are elaborated below.

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

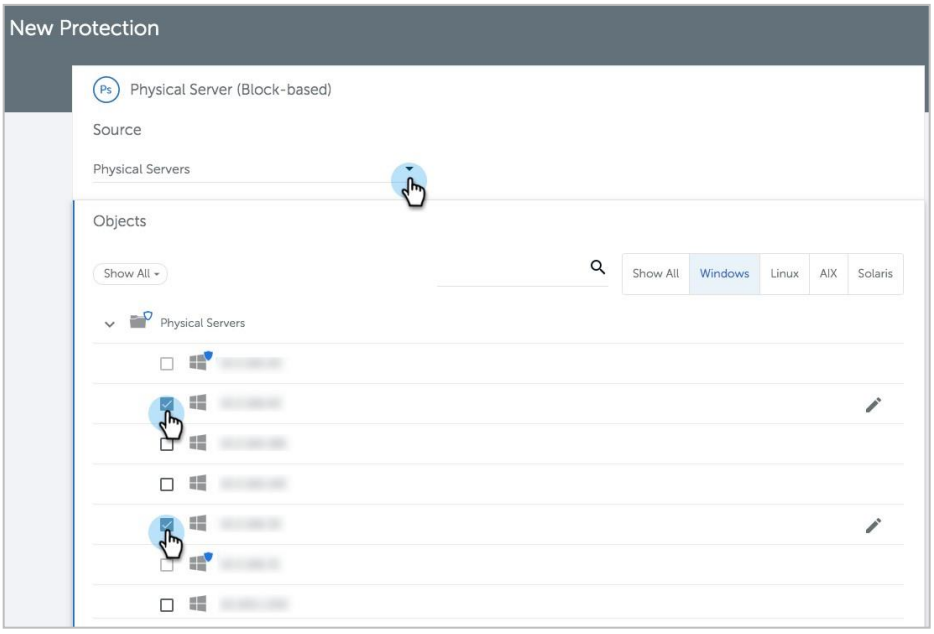
1. Navigate to **Data Protection** > **Protection**.



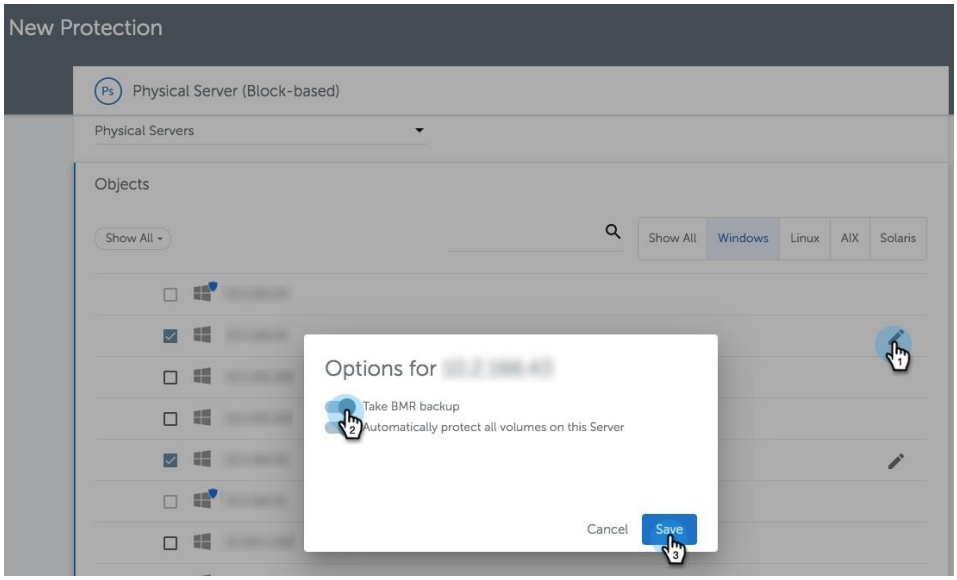
2. Click the **Add** button and select **Physical Server (Block-based)**.



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

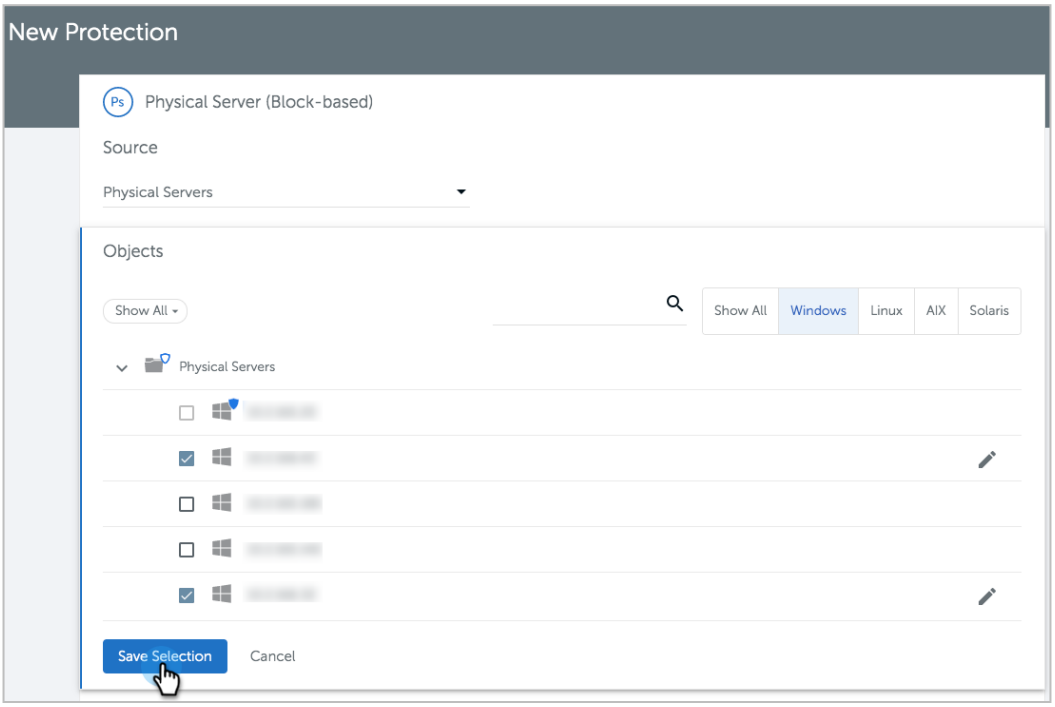


4. For each selected object, click the **Edit** button on the right and in the dialog, select **Take BMR backup** and click **Save**.

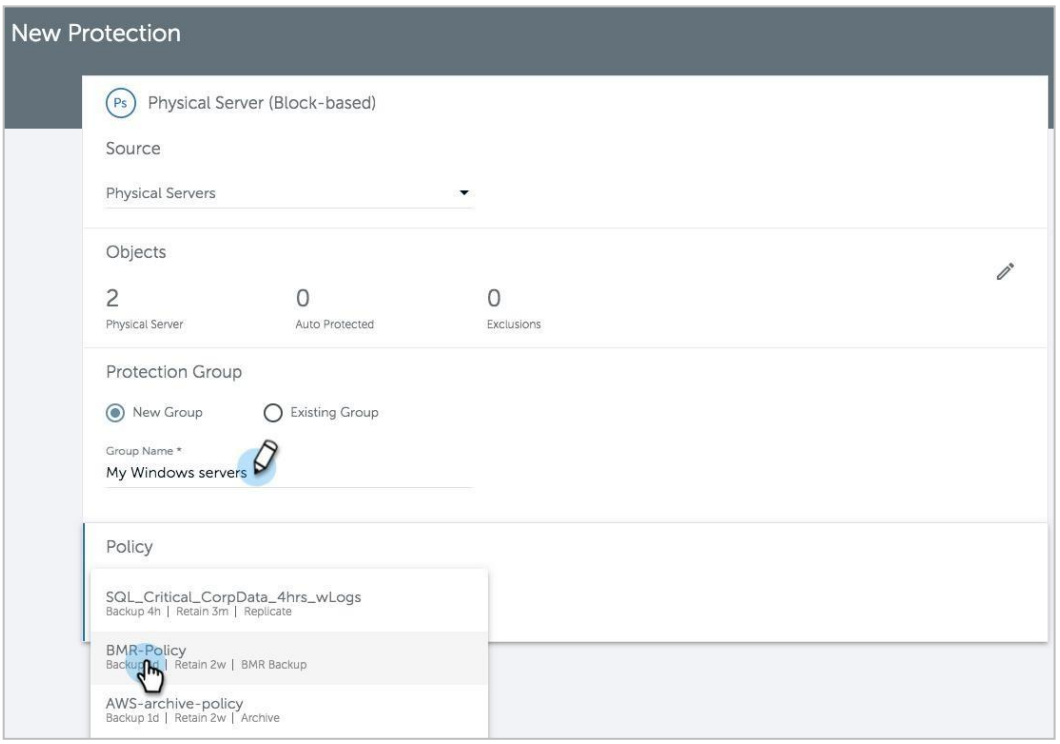


This step enables the Cohesity Agent for Windows to coordinate the entire physical server backup with the CBMR deployment service on the physical server.

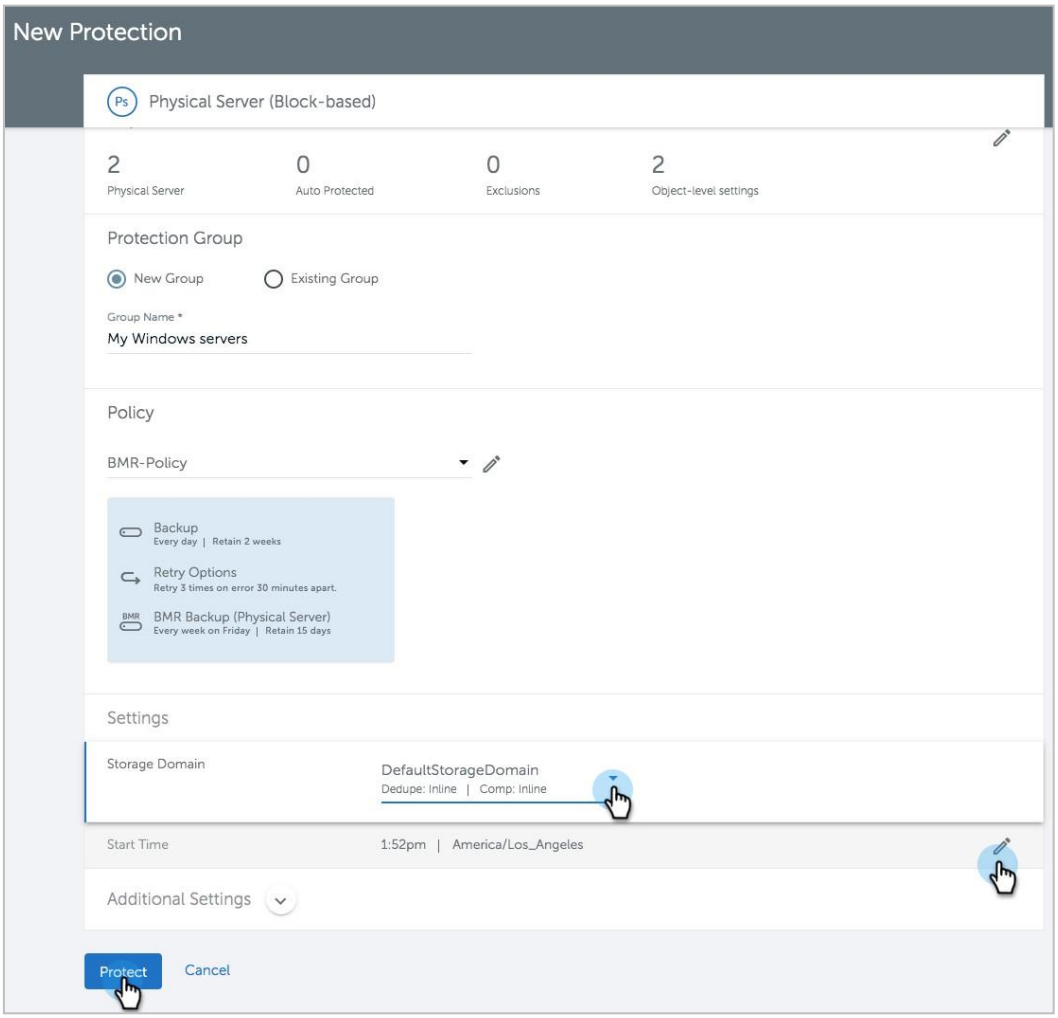
5. Once you have added the BMR backup to your source(s), click **Save Selection**.



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.

Create a Preinstallation Environment on Spare Server

Windows Preinstallation Environment (also known as Windows PE or WinPE) is a lightweight version of Windows with ready-to-boot environments. The Cristie Recovery ISO Producer (CRISP) software enables you to create a customized bootable WinPE recovery environment in an ISO image that works with CBMR and Cohesity.

To create a WinPE recovery ISO:

1. Install the Windows ADK.
2. Install CRISP.
3. Create the recovery ISO.

Install Windows ADK

The Windows Assessment and Deployment Kit (ADK) is a collection of tools that are designed to help deploy Microsoft Windows OS images to target machines. CRISP relies on the Windows ADK to build the recovery ISO image.

IMPORTANT: Figure out which WinPE version you will use to build the Cristie recovery ISO. This willdetermine the version of the Windows ADK.

- For WinPE version 5 (on Win8.1 to Win2012R2), use the Windows ADK version 8.1.
- For WinPE version 10 (on Windows Server 2008 R2 to Windows Server 2019), use the WindowsADK version 10 v.1903.

To install the Windows ADK, see Download and install the Windows ADK in the Microsoft documentation.

Install CRISP

Cristie Recovery ISO Producer (CRISP) is a tool that is bundled with the CMBR suite. With CRISP, a user can create a customized recovery ISO. CBMR uses this ISO to boot an environment to recover the system from a Custom Virtual Device Driver (.vtd) file. The creation of bootable recovery ISO is a one-time task, and this ISO can be used to recover any number of Windows servers. It is not necessary that CRISP & Cristie BMR be installed on the same server.

For the guidelines and requirements for using CRISP, see How to perform a Cristie bare machine recovery (CBMR) for physical Windows servers in the Cohesity Support portal.

To begin the CRISP installation:

1. Run the CBMR Suite installation binary. Follow the prompts to select your language, accept the License Agreement, and select **Install CBMR Suite**.

2. In the **Select install component** dialog that appears, select Install **CRISP and the Fileset**.

3. Select a location and click **Install**.
4. When the process completes, click **Finish** and reboot the server.

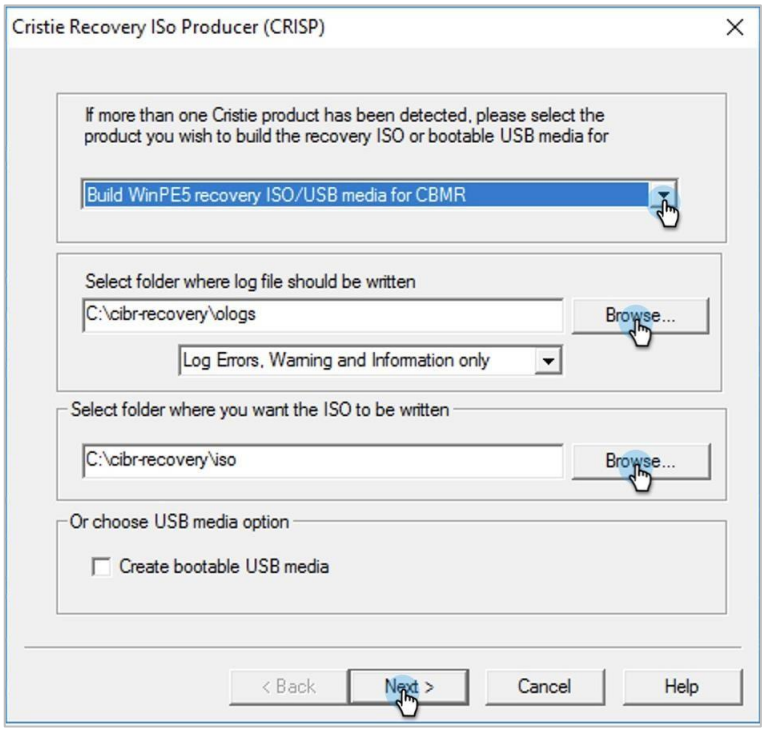
Create Recovery ISO

Now you're ready to use CRISP to create the recovery ISO. The recovery ISO provides a bootable image that is used in the CBMR recovery environment. Following best practices, you should create the recovery ISO image on a Windows server other than the server being backed up, to avoid a single point of failure.

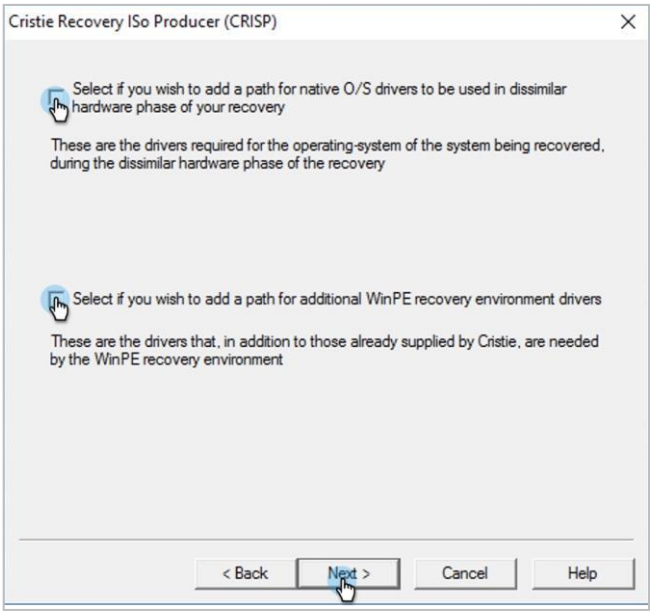
To create the recovery ISO:

1. Start CRISP from the Windows menu.

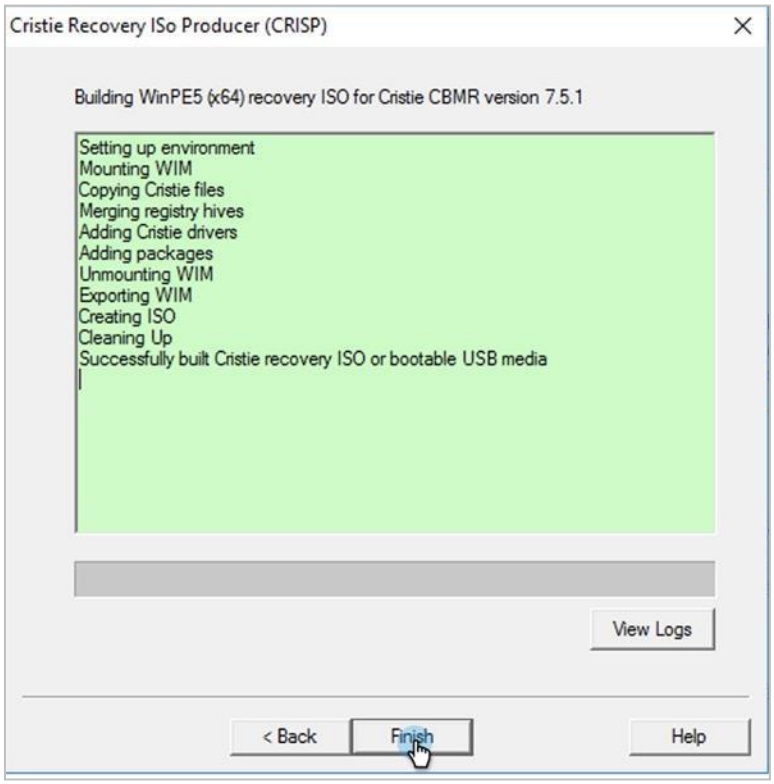
2. When CRISP prompts you, select the ISO fileset corresponding to the product for which you wish to build the WinPE environment. Select the folders where the log file and the recovery ISO will be written and click **Next**.



3. The next screen gives you the option to add additional drivers to be used when you are recovering onto dissimilar hardware. In those cases, check the box to **add a path for native O/S drivers**. You can also add additional WinPE drivers to support your recovery scenario if necessary. Choose your options and click **Next**.



4. In the next screen, select the options as necessary and click **Next** to start creating the recovery ISO.
5. When prompted, click **Finish** to complete the process.



TIP: Navigate to the folder you specified for the ISO image to confirm its creation.

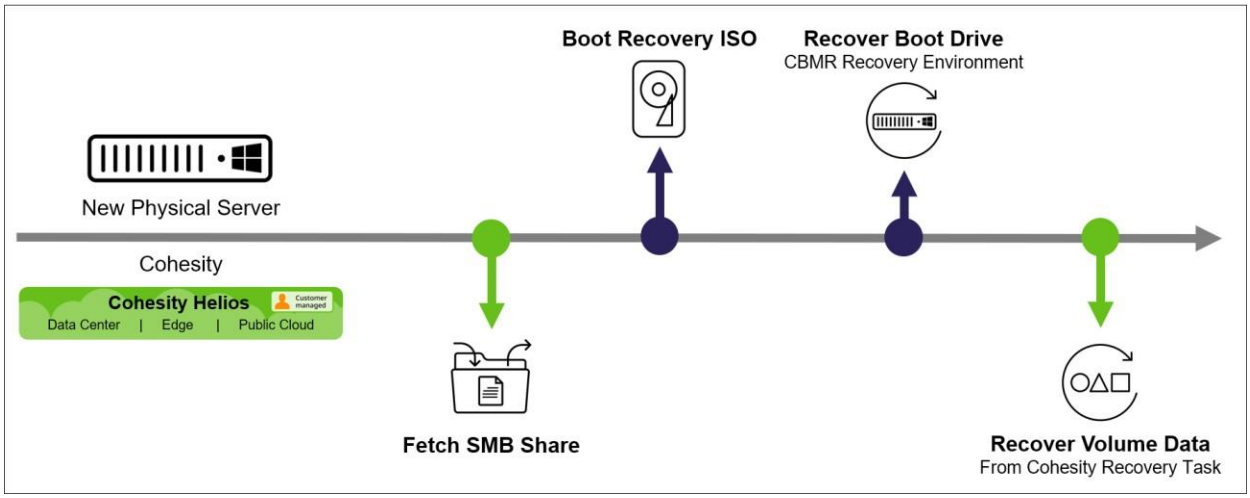
Recover Your Server Using Cohesity with CBMR

Cohesity facilitates the recovery of BMR backups, to both the original and alternate machines, at various degrees of granularity. During a BMR-enabled backup, the volumes and the system data are copied to Cohesity as Custom Virtual Device Driver (.vtd) files, to provide a seamless and a swift restore experience to the user. For a BMR recovery, the desired point-in-time state of the server is exposed as an SMB share. This SMB share is mounted while booting the recovery ISO to perform restoration of system data and volumes. The restore experience is hassle-free, fast, and automatic while preserving the integrity of the server. There is no need to install the OS, manually partition the disk, or set up the network.

There are several tasks involved in recovering your server:

1. Recover the server's boot drive.
    a. Fetch the SMB share from Cohesity.
    b. Boot the recovery ISO.
    c. Recover your server using the CBMR Recovery Environment.
2. Once the server is online, you can recover the volume data.

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.
- The Cohesity cluster is part of an Active Directory. To join a Cohesity cluster to an Active Directory,see Join Active Directory in the online Help.
- SMB Authentication is enabled.

Recover Your Server Boot Drive

The first step in recovering your server is to recover the boot drive. After that, you can recover the volume data, as described in the next section.

To recover your server's boot drive:

1. Fetch the SMB share from Cohesity.
2. Boot the recovery ISO on a new bare machine or virtual machine.
3. Use the CBMR Recovery Environment to configure the network and use the Cristie recovery wizard.

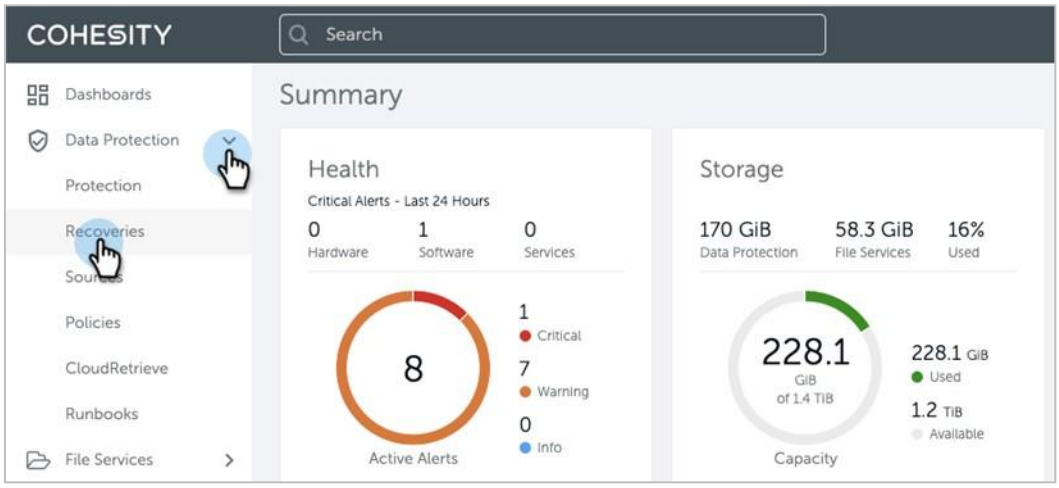
Fetch the SMB Share from Cohesity

To access the recovery ISO you created, you'll need to fetch the complete SMB share from Cohesity. This is a two-step process.

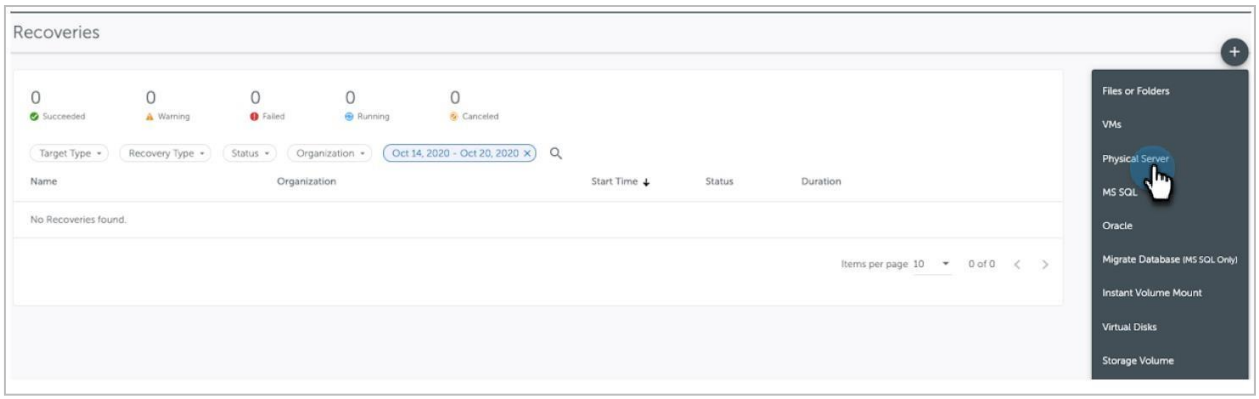
1. Get the unique recovery path that reveals the folder information.
2. Mount the unique recovery path temporarily to get the complete path that will be used by the recovery ISO.

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

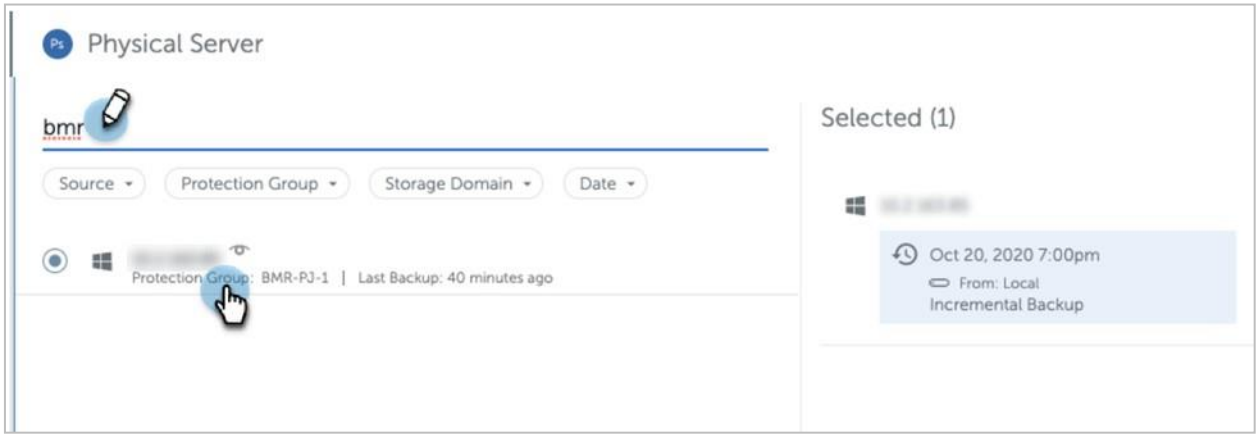
1. Log in to Cohesity.
2. Navigate to **Data Protection** > **Recoveries**.



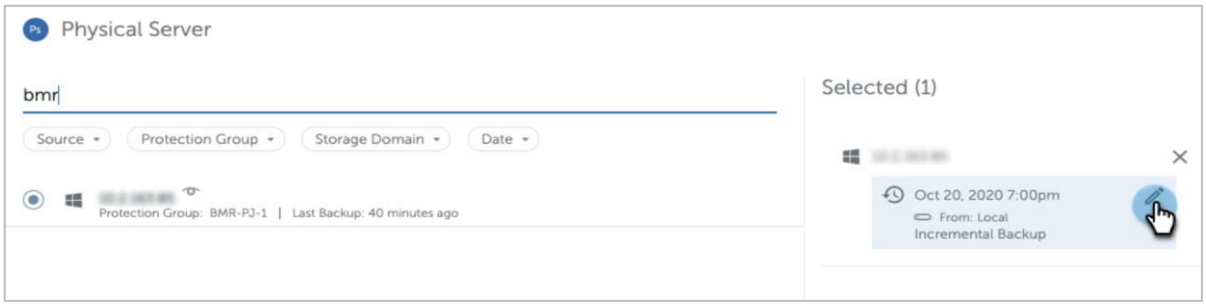
3. Select **Recover** > **Physical Server**.



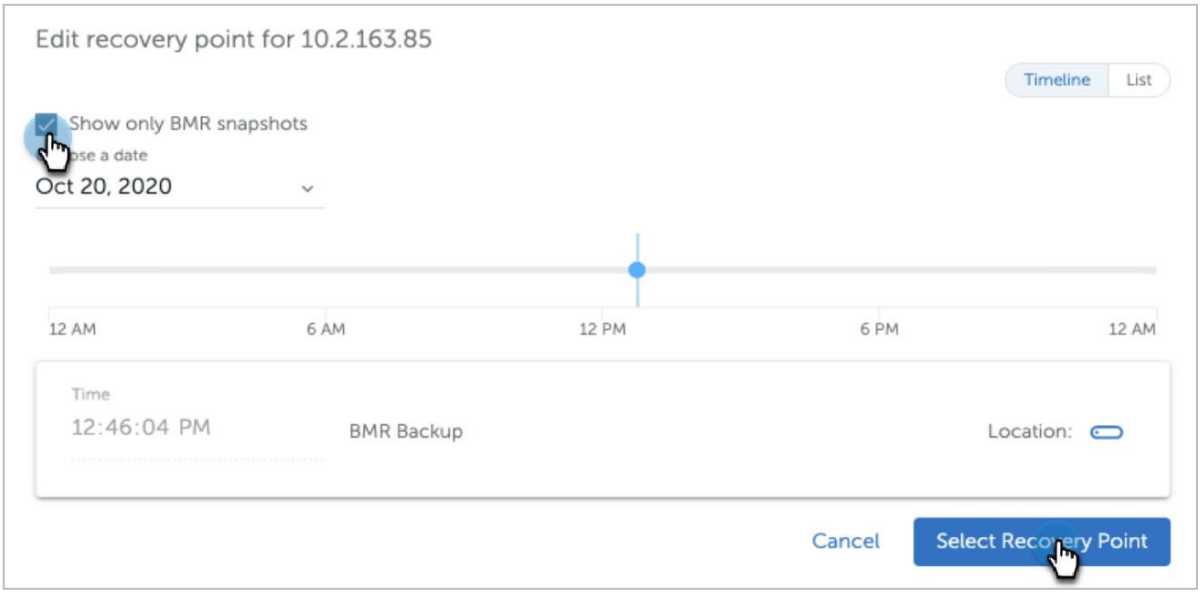
4. Enter a term to search by **Server or Protection Group Name**. In the search results, click the server you wish to recover.



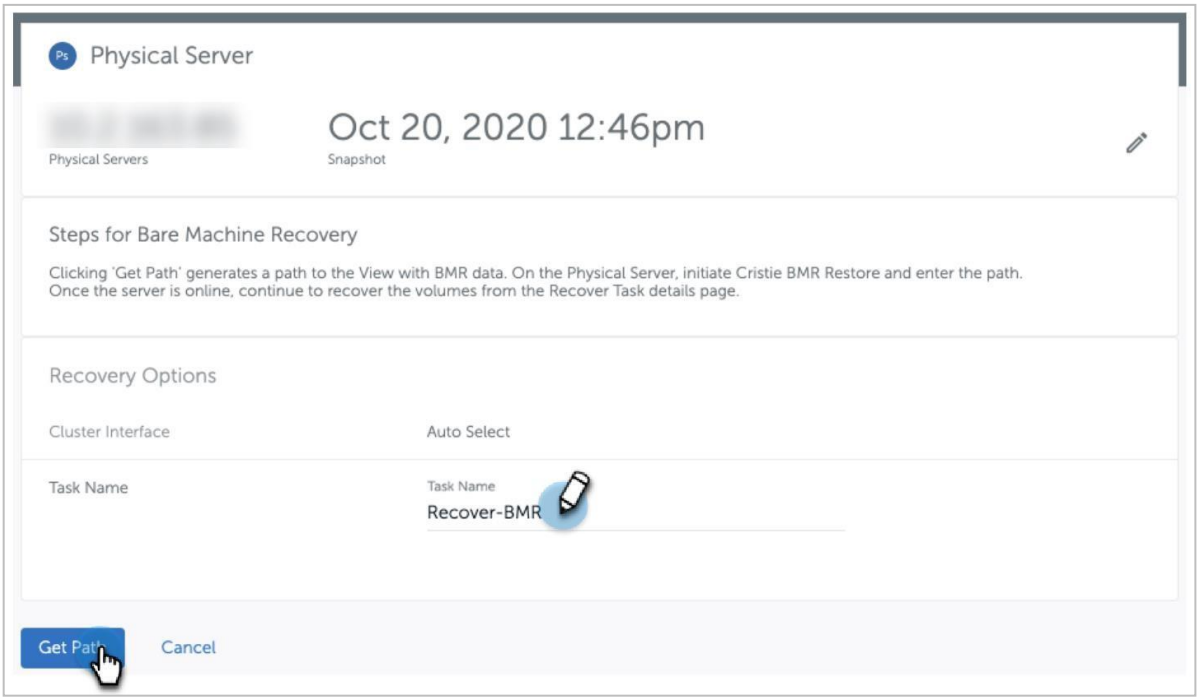
5. Select the BMR Recover Point, click the **Edit** (pencil) icon.



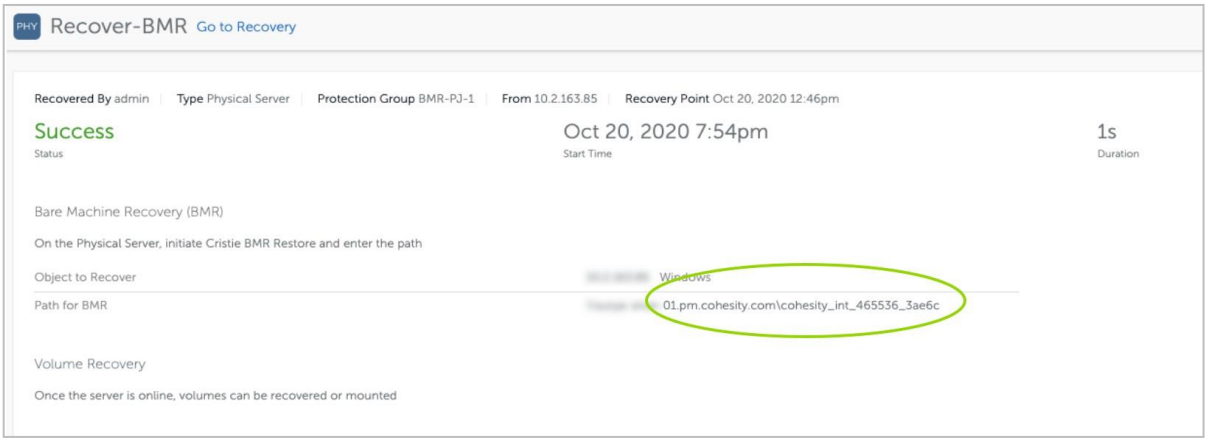
6. Check the **Show only BMR snapshots** option, choose a recovery point, and click **Select Recovery Point**.



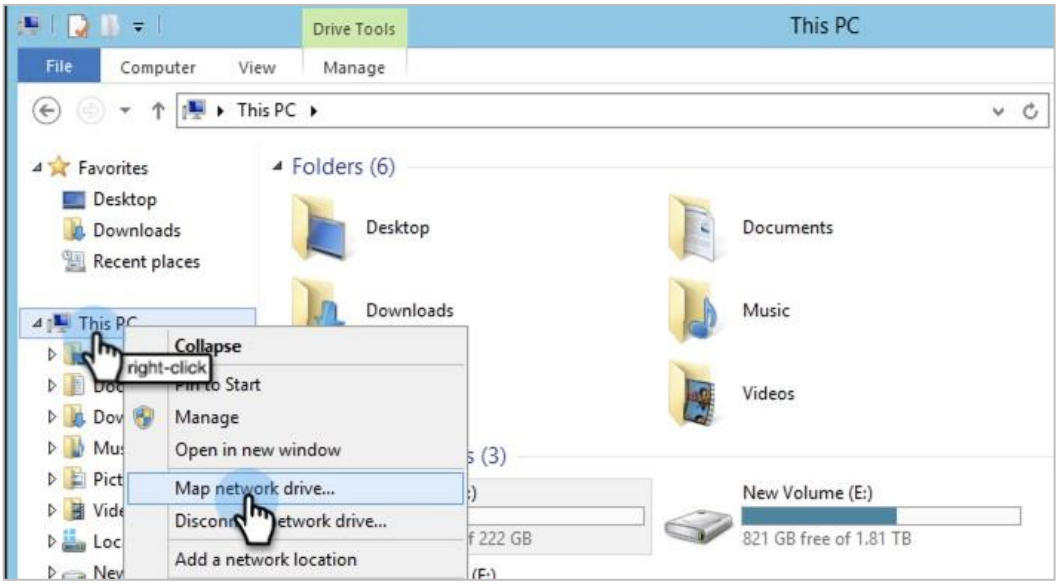
7. Accept the auto-generated **Task Name** or enter a new one if you wish to and click **Get Path** to reveal the SMB share path.



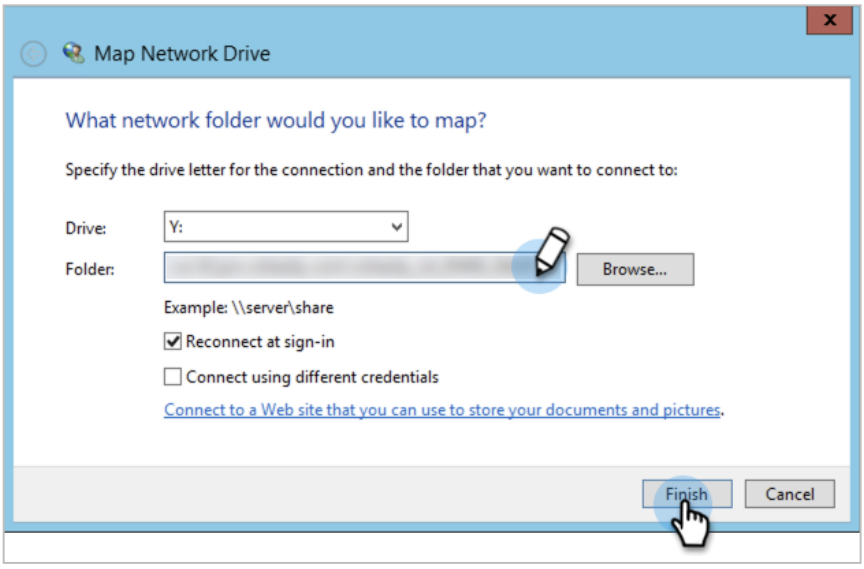
8. After a few moments, the **Path for BMR** appears. This is the SMB share path that you will mount in the Cristie recovery wizard. Copy the SMB share path and save it.



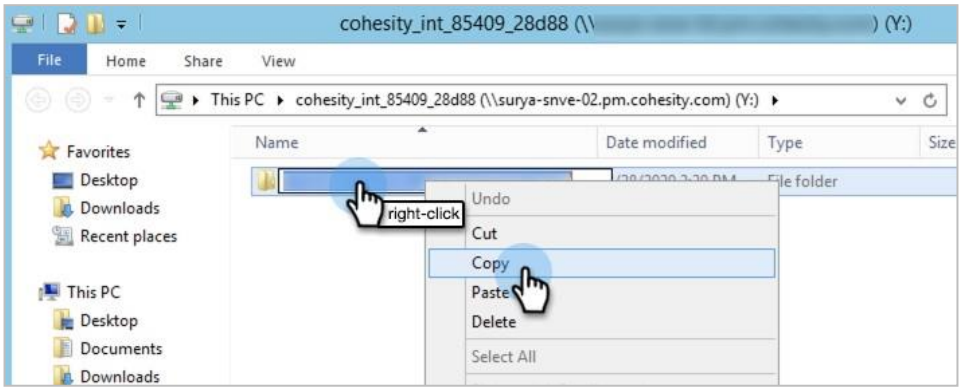
9. On your spare Windows server, open Windows Explorer, right-click **This PC**, and select **Map network drive…**



10. Paste the SMB share path that you captured above into the **Folder** field and click **Finish** to mount the SMB share on the Windows machine. If you are prompted for credentials to access the SMB share, enter them.



11. In the SMB share folder, copy the subfolder name.



12. Append the subfolder name to the SMB share path to get the full path you will use to recover the server on a new machine or VM.

    For example, if the SMB path is ***test.bmr.com*** and subfolder is ***17504_156_9341***, then the complete recovery path is ***test.bmr.com\17504_156_9341\system.vtd***.

    You are now ready to boot the recovery ISO.

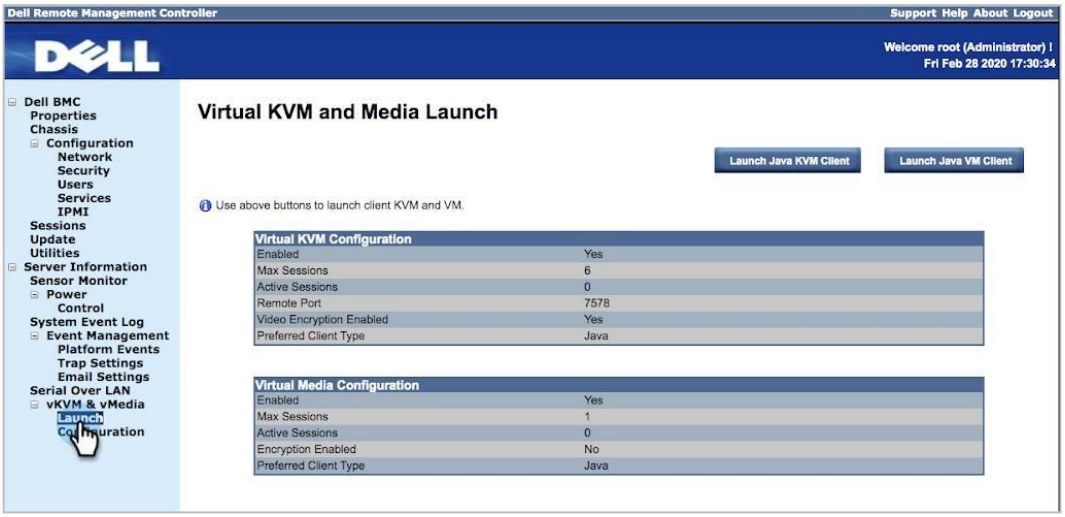
Boot the Recovery ISO on New Bare Machine

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 remote controller 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.

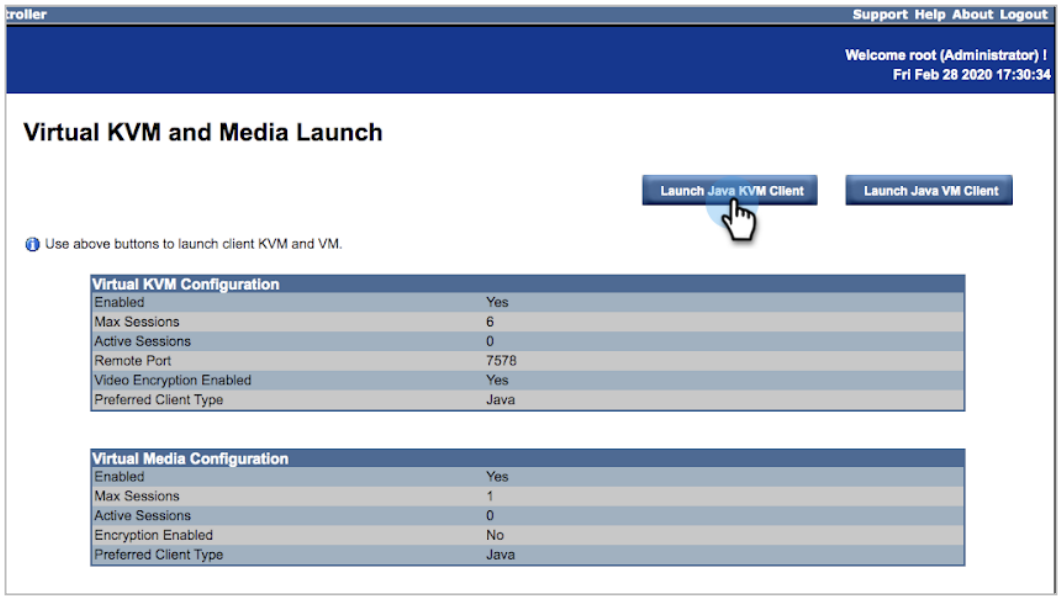
NOTE: This process involves recovering your server onto a new bare machine (P2P), but you can alsorecover it onto a VM (P2V). See Boot the Recovery ISO on a VM.

To boot the ISO on a new bare machine:

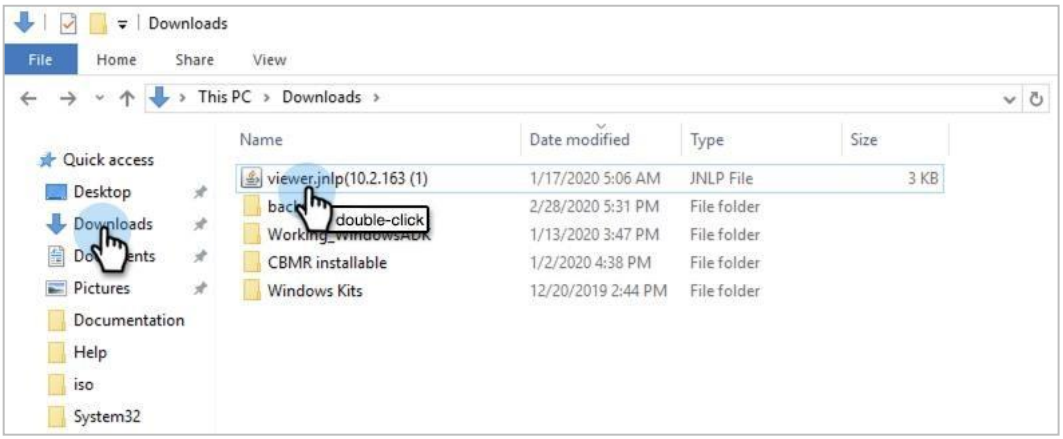
1. Log in to the Remote Management Controller of the new bare machine. Navigate to **Server Information** > **Serial Over LAN** > **vKVM & vMedia** > **Launch**.



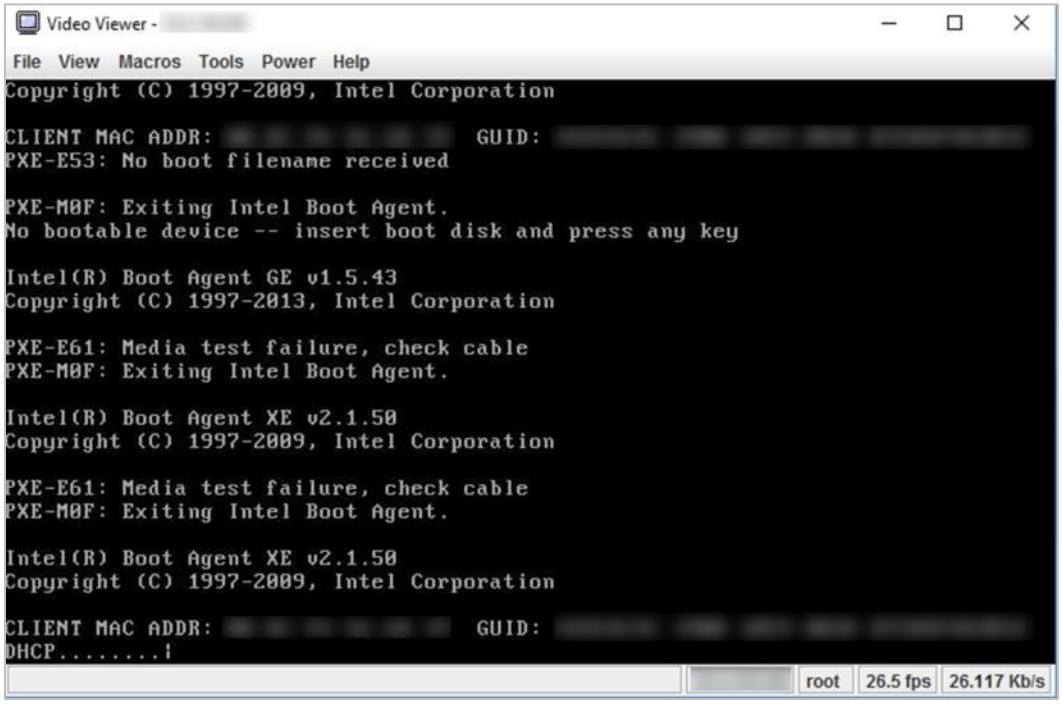
2. Click **Launch Java KVM client**.



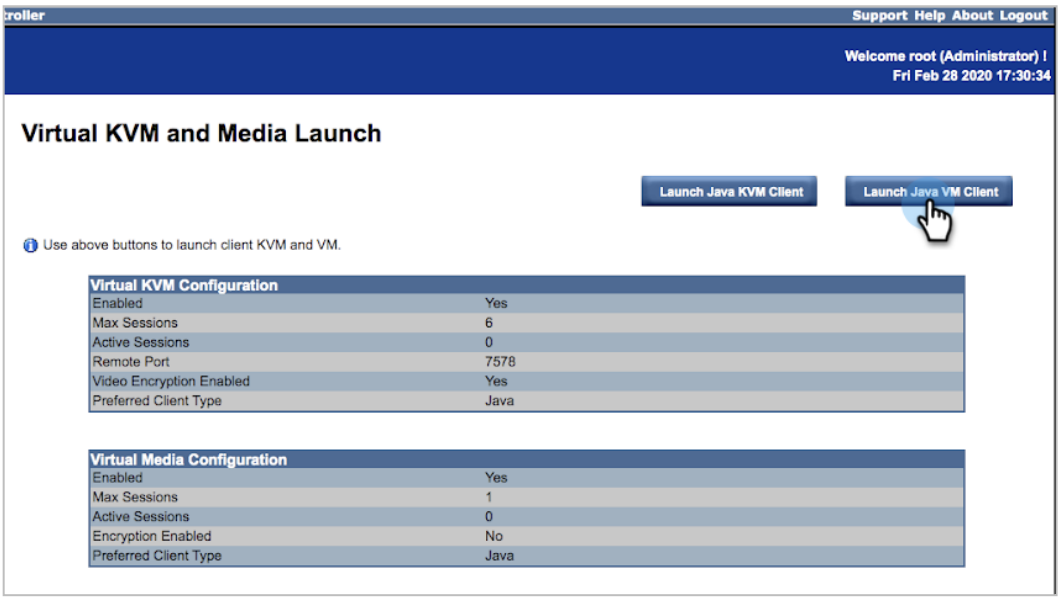
3. This downloads a Java Network Launching Protocol (JNLP) file, which you can use to launch a KVM session. Launch the `.jnlp` file to start the KVM session.



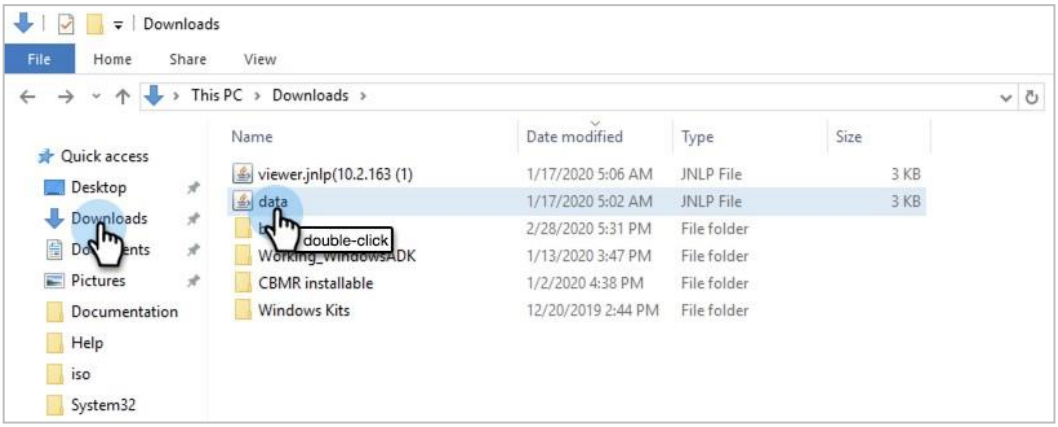
4. A video viewer running the KVM session opens.



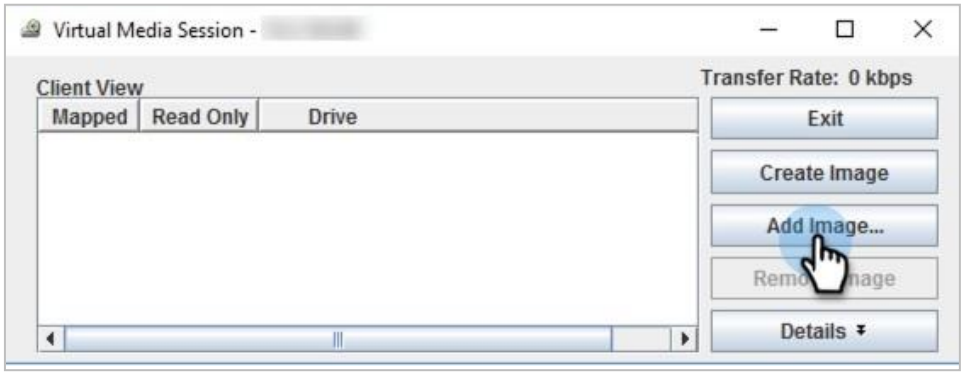
5. Return to the Remote Management Controller and click **Launch Java VM Client**.



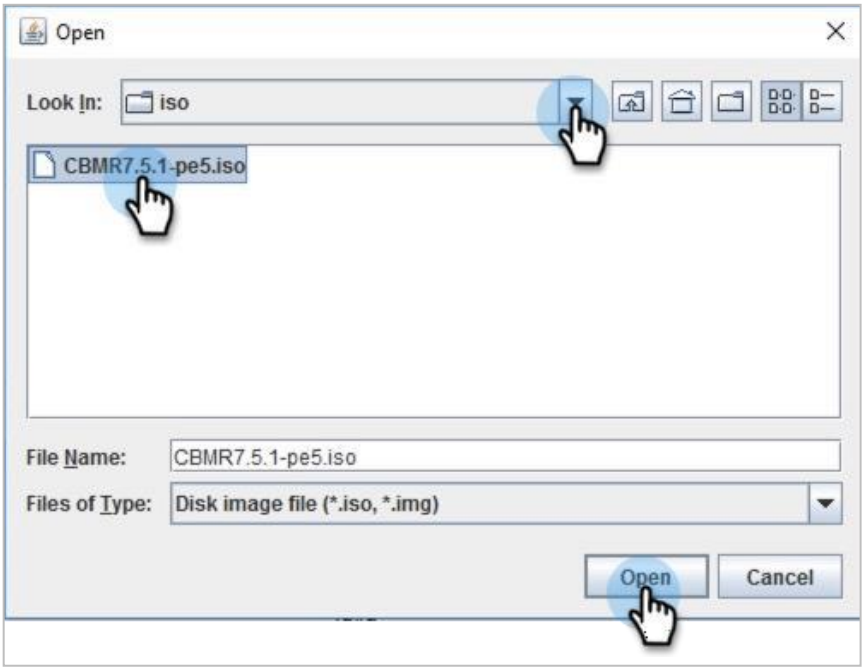
6. This downloads another `.jnlp` file called '`data`.' Double-click this file to launch a Virtual Media Session.



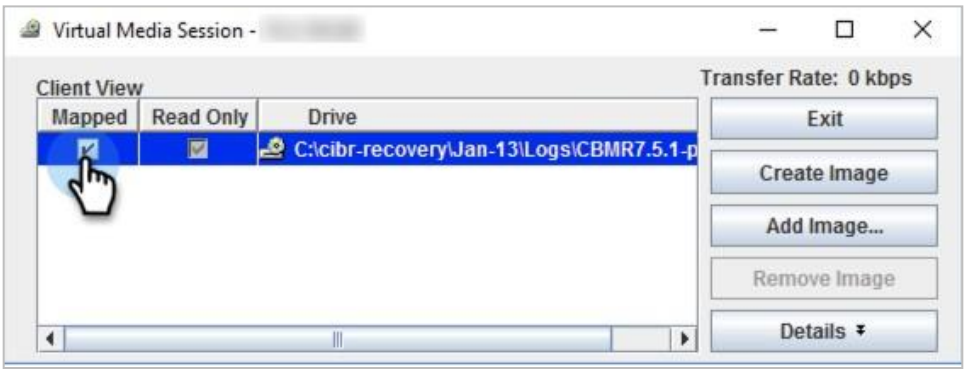
7. A Virtual Media Session opens. Click **Add Image**.



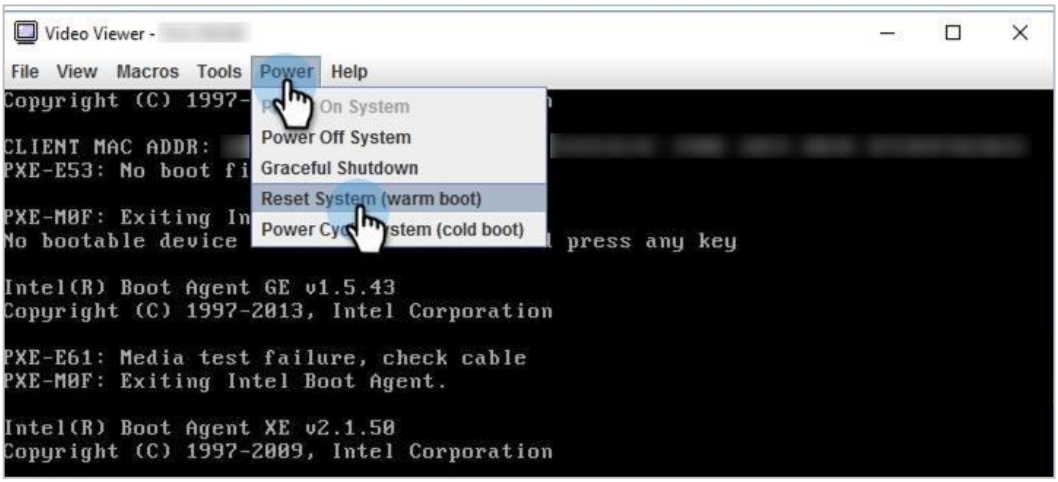
8. Navigate to [the folder where CRISP saved the ISO image]. Select the recovery ISO and click **Open**.



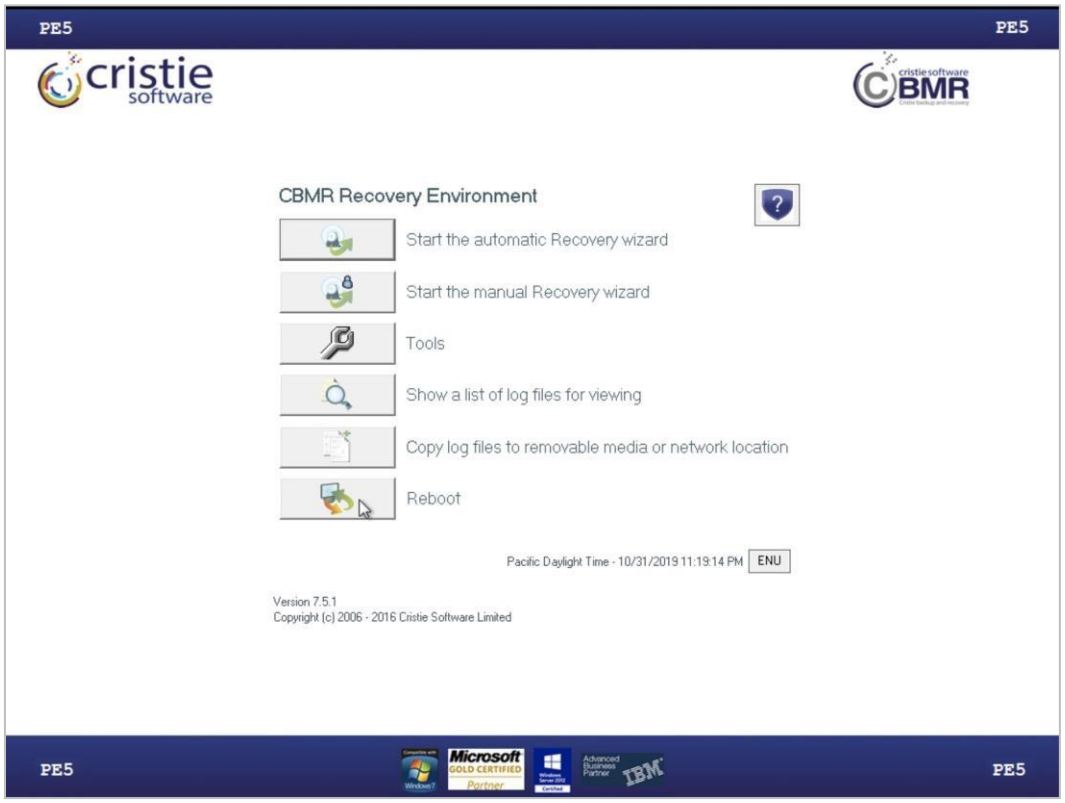
9. Check **Mapped** to map the recovery ISO to the target host.



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



11. On KVM reboot, the mapped ISO image is loaded and the Cristie recovery wizard opens.



To continue, go to Use the CBMR Recovery Environment.

Boot the Recovery ISO on a VM

The recovery process is very similar for 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 starts a 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 a Windows installation-like boot procedure. During the boot process, the WinPE5 or WinPE10 driver for your plug-and-play devices is loaded and the CBMR Recovery Environment opens.

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

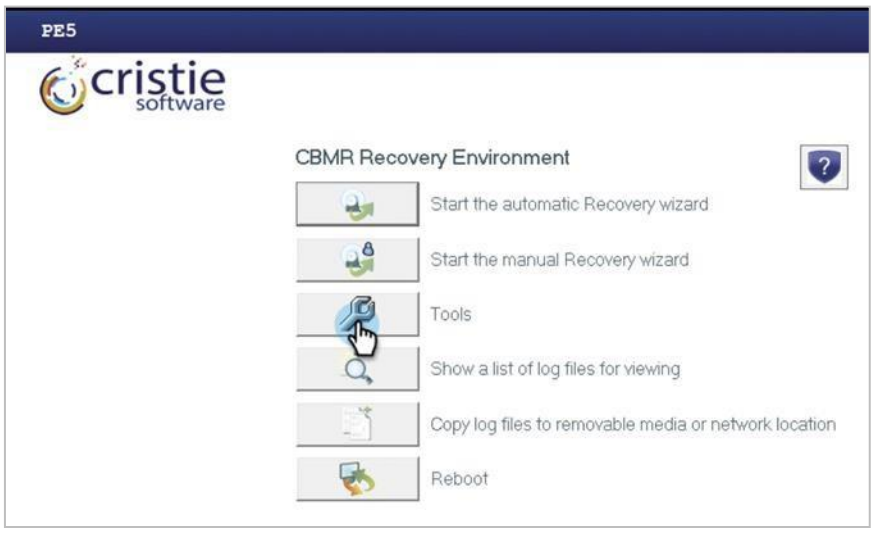
1. Configure the network to access the SMB share exposed from Cohesity.
2. Use the recovery wizard to initiate recovery.

Configure the Network

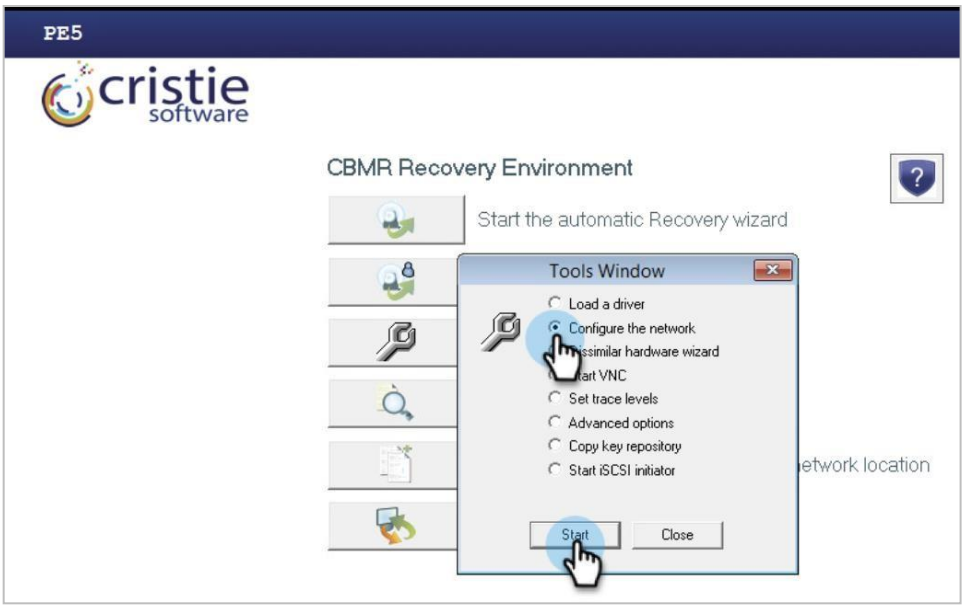
The server marked for recovery must be configured in the network to access the SMB share from Cohesity. We recommend that you configure the network before you initiate the automated recovery.

To configure the network for recovery:

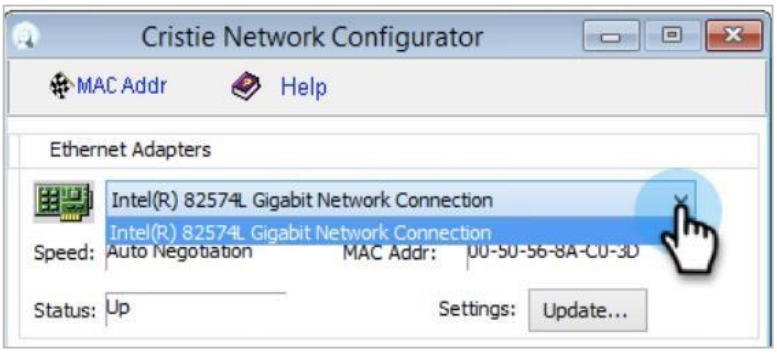
1. From the CBMR wizard, click **Tools**.



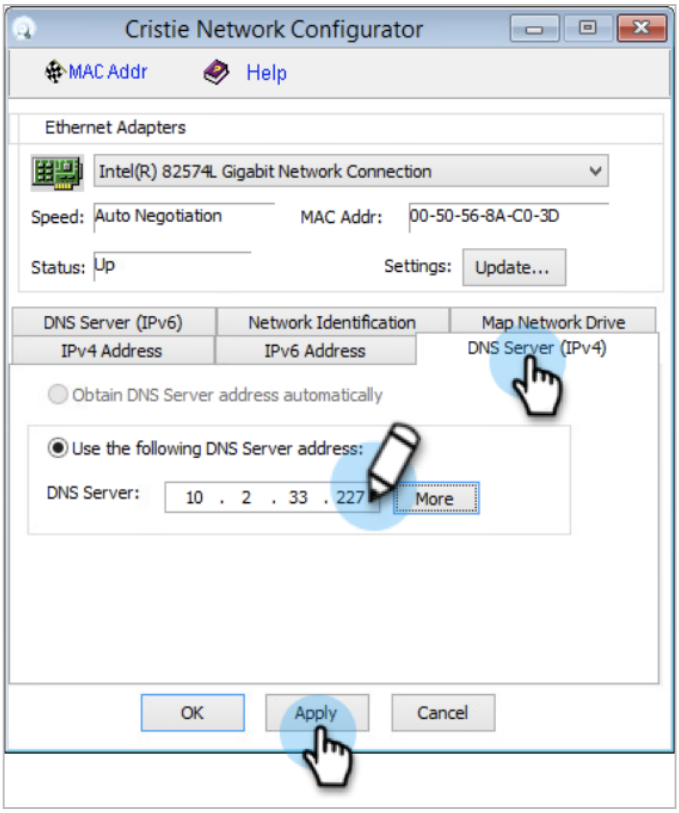
2. From the **Tools Window**, select **Configure the network** and click **Start**.



3. In the **Cristie Network Configurator**, select your preferred adapter.



4. Click the **DNS Server (IPv4)** tab to enter the preferred DNS and click **Apply**.



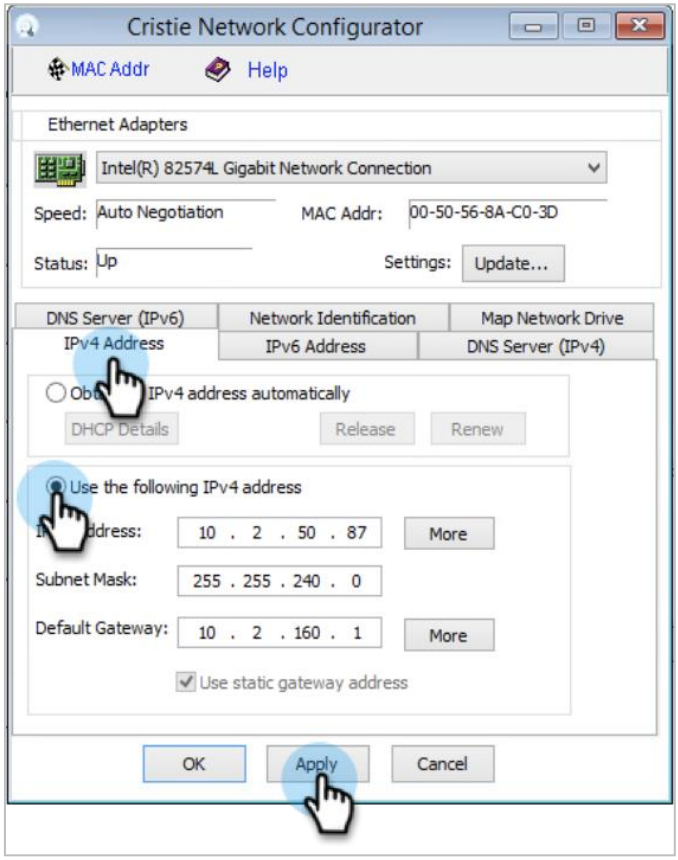
5. Click the **IPv4 Address** tab to configure the network to a static IP address and gateway. You have two configuration options:

   a. **DHCP**: Choose **Obtain an IPv4 address automatically** for dynamic IP address allocation.

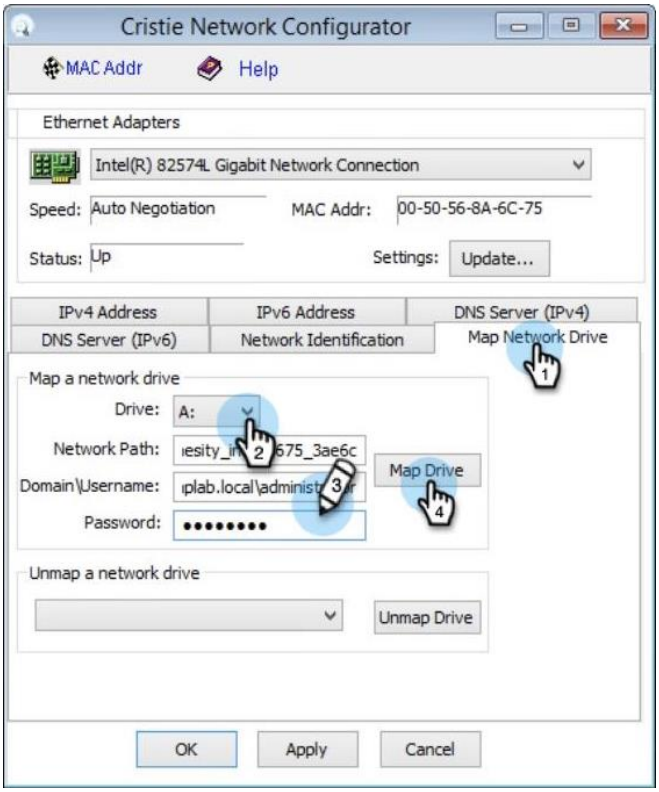
   b. **Manual**: Choose **Use the following IPV4 address** and enter a valid IPv4 **Address**, **Subnet Mask**, and **Default Gateway**.

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

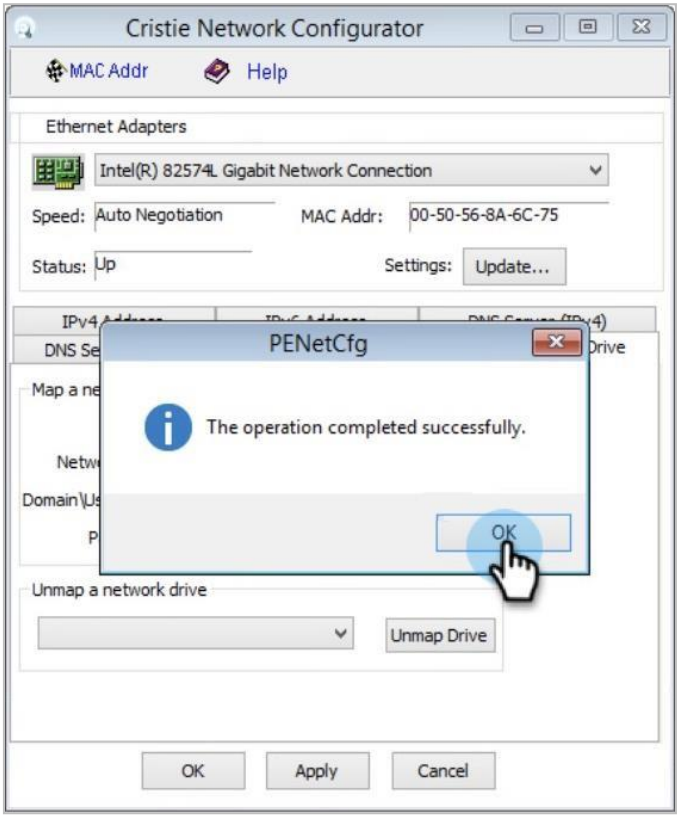
   Click **Apply**.



6. Click the **Map Network Drive** tab to mount a network share to the CBMR Recovery Environment. Enter the parameters as specified and click **Map Drive**.
   a. **Drive**: Choose the drive to map.
   b. **Network Path**: Enter the unique recovery path you fetched from Cohesity.
   c. **Domain\Username**: Enter the domain and user to authenticate the drive.
   d. **Password**: Enter the domain user's password.



7. Click **OK** to complete network configuration.



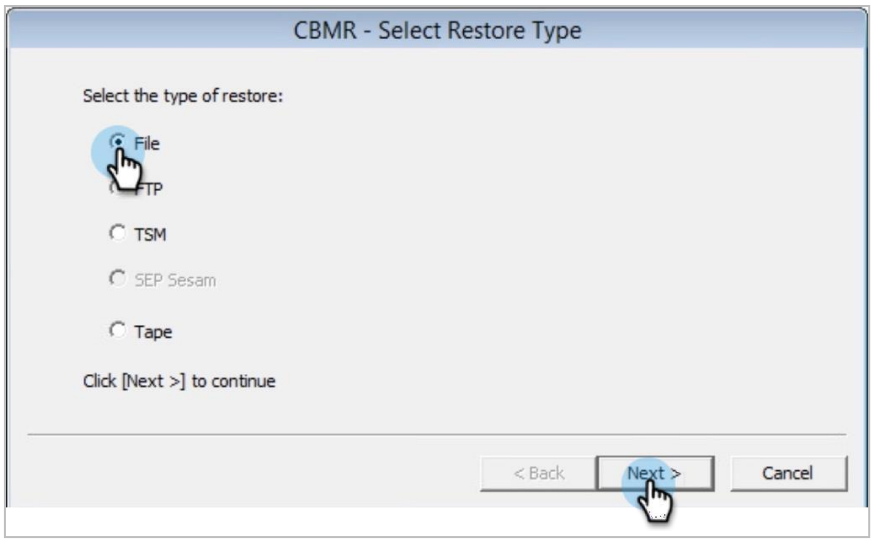
Use Recovery Wizard to Initiate Recovery

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

To initiate recovery:

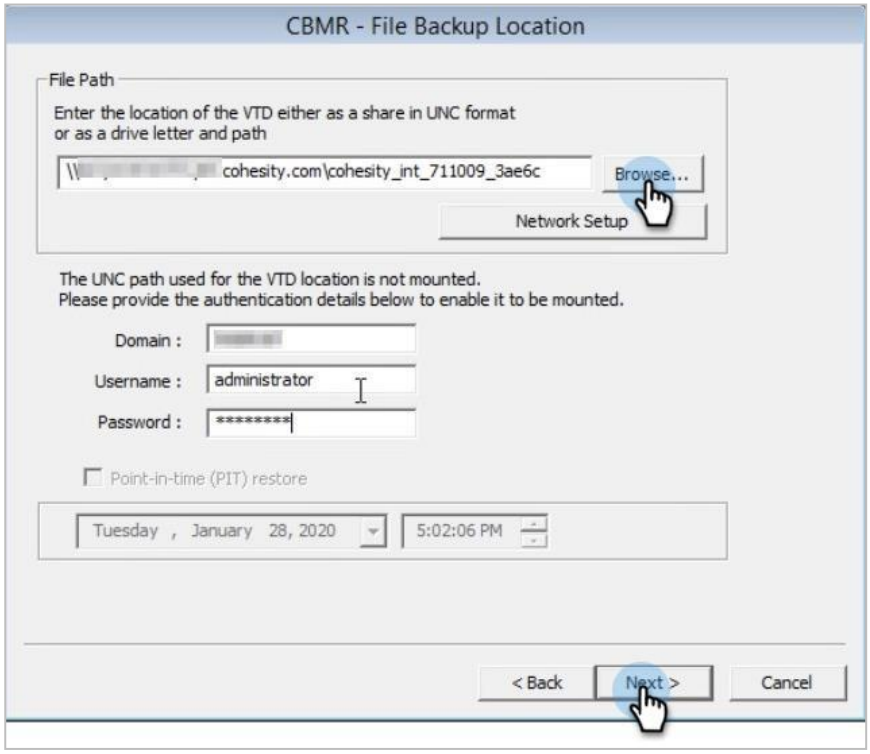
1. In the CBMR wizard, click **Start the automatic Recovery wizard**.

2. Select **File** and click **Next**.



3. In the following page, you are prompted to enter the location to the Custom Virtual Device Driver (.vtd) file. There are three ways to enter the location:

   If a network drive is mapped, click **Browse** and navigate to the mapped drive and select the `system.vtd` file. (If you have not mapped the drive, you can enter the path you fetched above directly.)

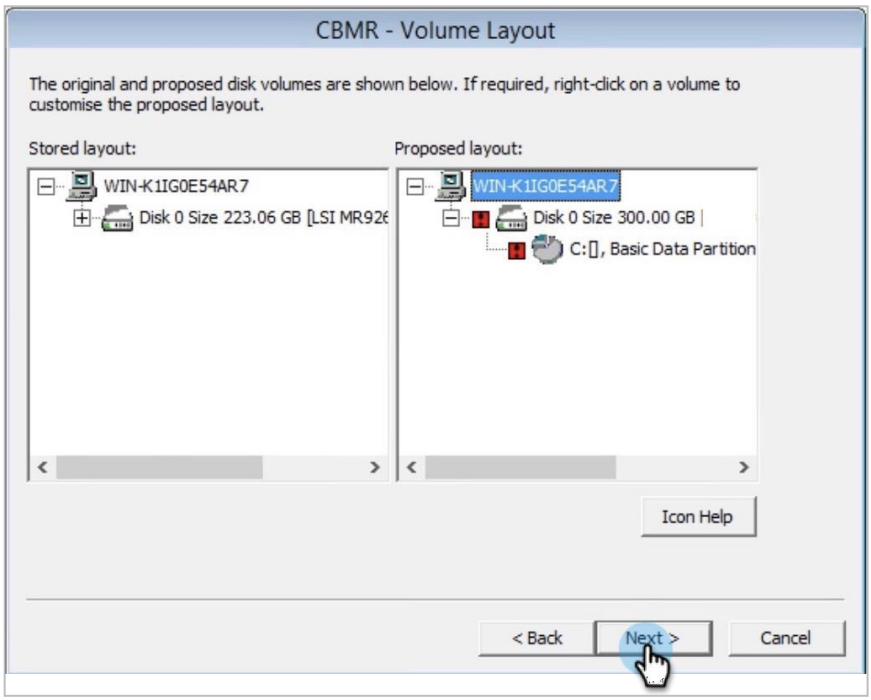


   Click **Next**.

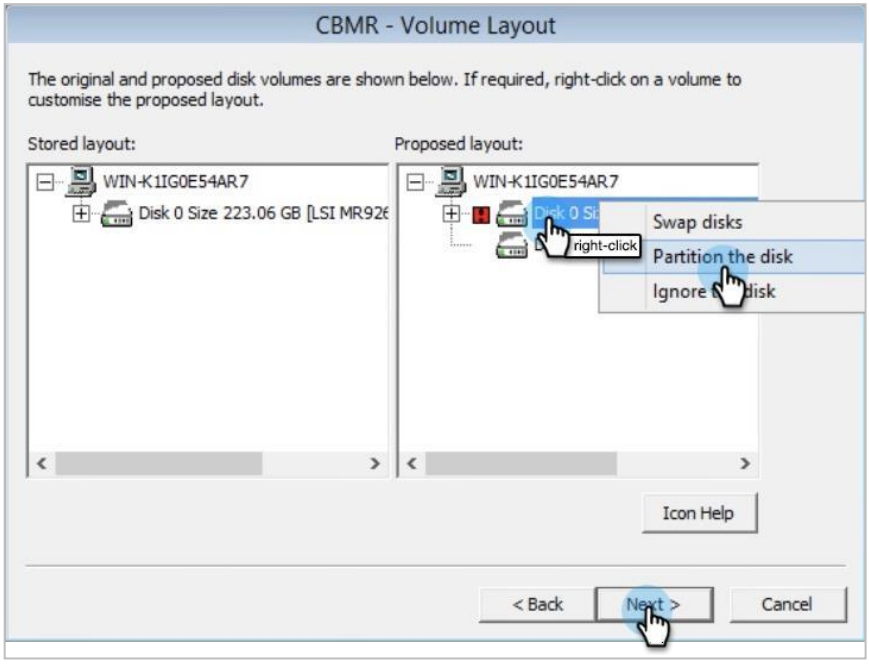
4. The recovery wizard connects to the local recovery client and starts reading both the system files and volumes.

5. After successfully connecting to the recovery client, the wizard presents a list of disks and partitions to be recovered in the CBMR Volume Layout dialog. Proceed with one of the two scenarios:

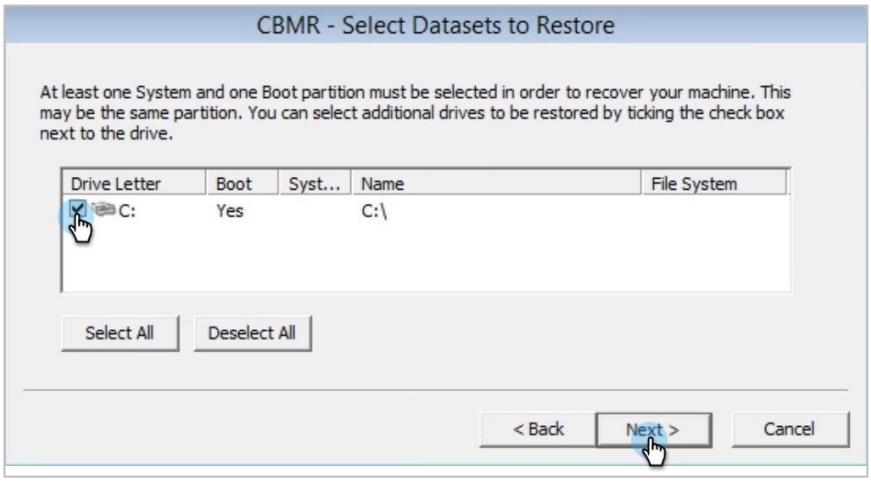
   a. **Similar Volume Layout**: If the recovery is back to the original server or a different server with the same volume layout (similar hardware), the disk mapping is similar. You can select the **Proposed layout** and click **Next**.



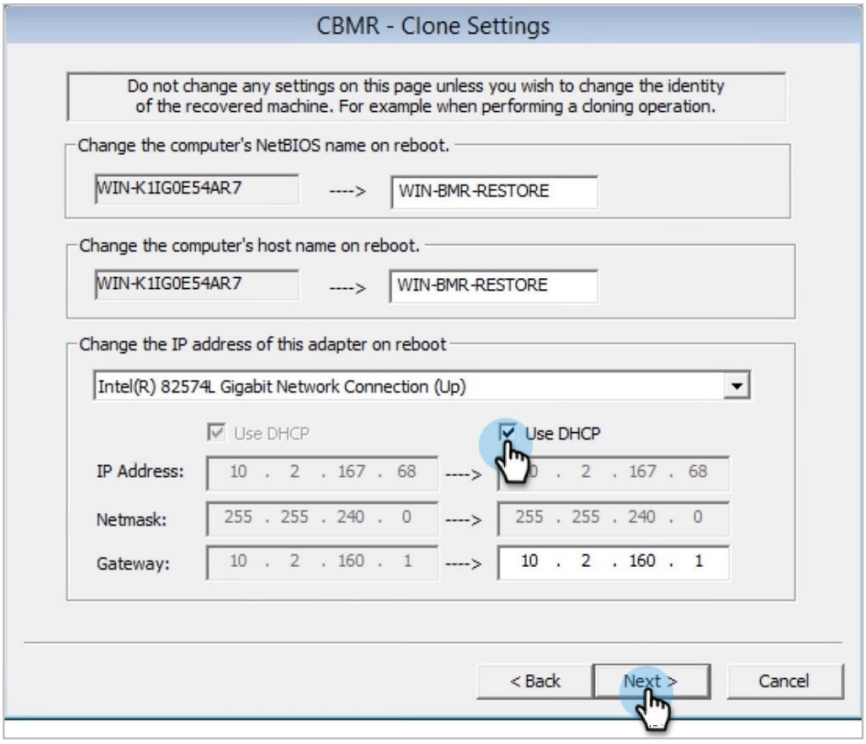
   b. **Dissimilar Volume Layout**: When recovering to a different server (dissimilar hardware), the mapping is complex with the different disk geometry and capacity. In such cases, you can right-click the disk shown under **Proposed layout** to select the disk to be partitioned or not. Then click **Next**.



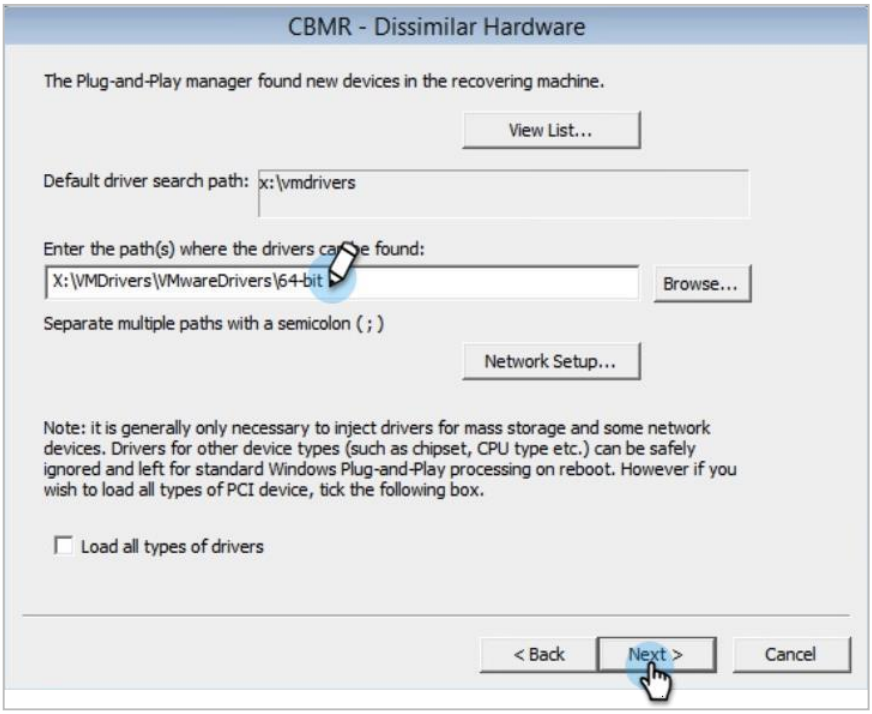
6. In the following screen, select the datasets to restore and click **Next**.



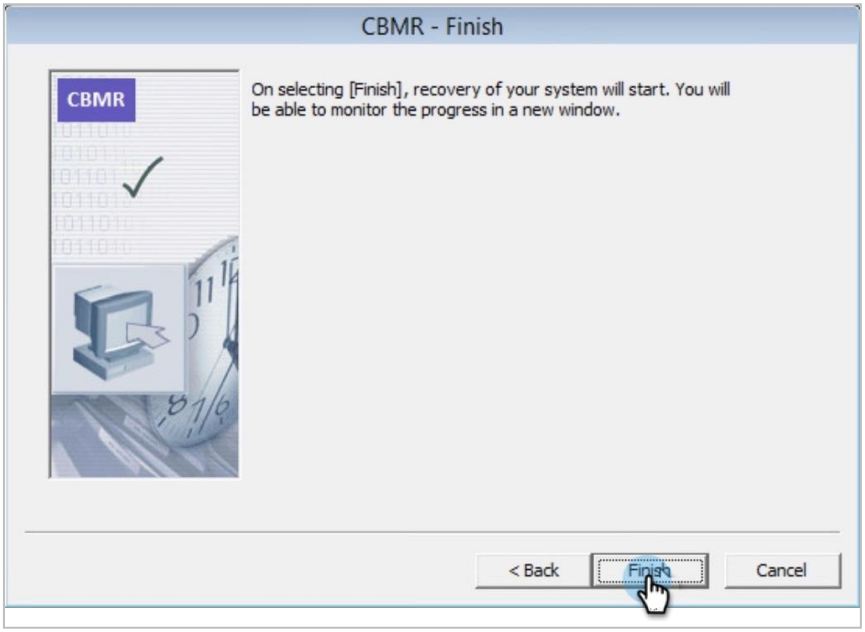
7. Use the **Clone Settings** dialog to set the target hostname and IP address. You can **Use DHCP** or enter a valid static IP address. Click **Next**.



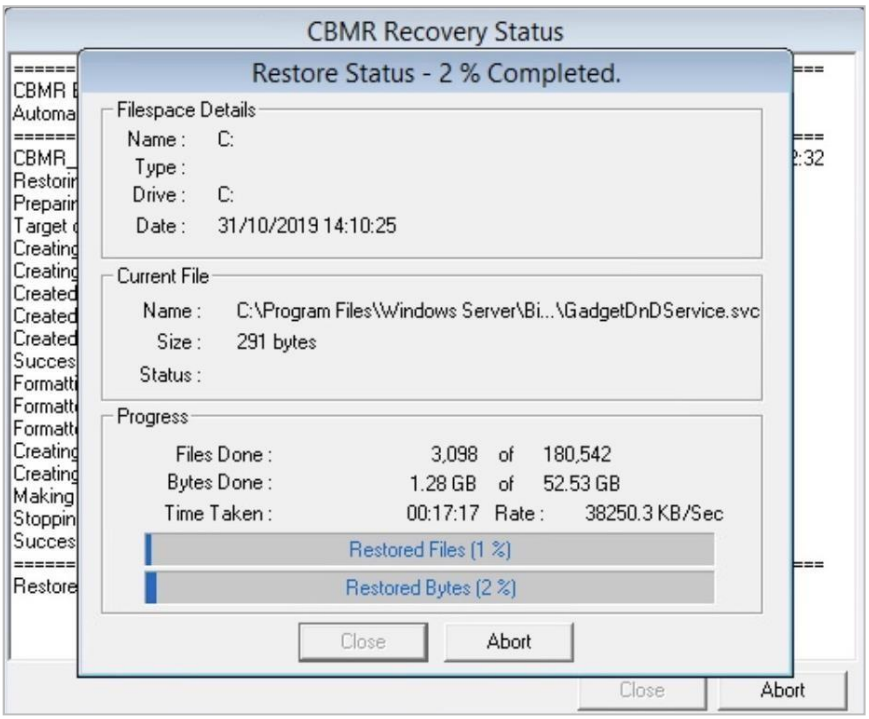
8. If you are restoring a Windows server to a dissimilar hardware, the Dissimilar Hardware component of the recovery wizard allows you to inject new drivers. Enter the path of the drivers and click **Next**.



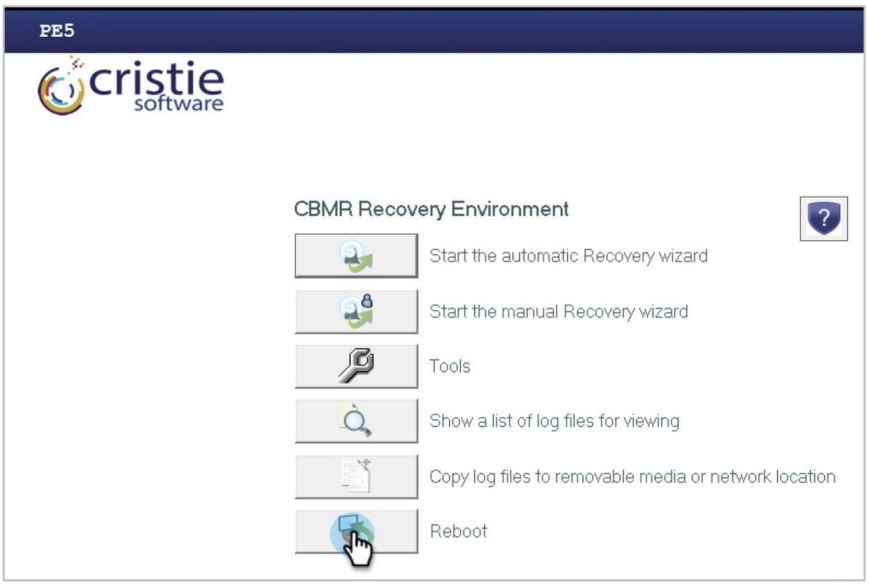
9. Click **Finish** to start the recovery.



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



11. After the recovery is complete, the system files, the source registry, and the user volumes are restored. Click Reboot to complete the recovery.



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

Recover Your Server Volume Data

Now that you have recovered the boot drive of your server, you are ready to recover the server's volume data from the same Protection Group that protects the boot drive.

To recover your server's volume data:

1. Log in to Cohesity and follow the first five steps in Fetch the SMB Share from Cohesity above.
2. Select your desired Cohesity Incremental snapshot and click Select Recovery Point.

3. From there, follow the instructions under **Perform Physical Volume Recovery** in Set Physical Server Recovery Options in the online Help.

You did it! You recovered and restored your server onto a bare machine, and it's ready to pick up where it left off. Go have a cup of coffee!

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 their documentation:

- Cristie Registration
- Windows CBMR licensing
- 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

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	Mar 2020	First release
1.1	Nov 2020	Update for 6.5.1
1.2	Dec 2020	Minor updates

ABOUT COHESITY

Cohesity ushers in a new era in data management that solves a critical challenge facing businesses today: mass data fragmentation. The vast majority of enterprise data — backups, archives, file shares, object stores, and data used for dev/test and analytics — sits in fragmented infrastructure silos that makes it hard to protect, expensive to manage, and difficult to analyze. Cohesity consolidates silos onto one web-scale platform, spanning on-premises, cloud, and the edge, and uniquely empowers organizations to run apps on that platform — making it easier than ever to back up and extract insights from data. Cohesity is a 2019 CNBC Disruptor and was named a Technology Pioneer by the World Economic Forum.

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