
Physical-to-Virtual Recovery

<https://campus.barracuda.com/doc/79463666/>

You can use the physical-to-virtual recovery (P2V) method to recover entire physical Microsoft Windows systems to a VMware or Hyper-V environment in the event the system has completely failed and no other recovery options are available. With P2V, all data, settings, applications, and operating system are installed to a VMware or Hyper-V system with no operating system installed.

To perform a P2V, all system volumes and the system state must be backed up on the data source. P2V requires that the target virtual system is configured with similar virtual hardware to the originally backed up physical system (source).

Windows 2016 and 2019 ReFS partitions are currently not supported in a physical-to-virtual restore.

Install the Windows ADK and Windows PE Add-On

The Barracuda Backup Bare Metal Recovery (BMR) kit is used to create a bootable ISO based on WinPE. This enables you to perform a physical-to-physical (P2P) or physical-to-virtual (P2V) bare metal restore of your Microsoft Windows Server, without installing an operating system first.

Before you can build a BMR ISO, you must install the Windows ADK and the Windows PE add-on for the ADK. The scripts included in the Barracuda Backup BMR Kit uses this software to generate an ISO used for bare metal recovery.

The following files are required to build the BMR ISO:

- From Microsoft:
 - The latest Windows ADK
 - The latest Windows PE add-on for the ADK
- From Barracuda:
 - The **Barracuda Backup Bare Metal Recovery Kit**. Within Barracuda Backup, navigate to the **System > Software Downloads** page and download from the **Windows Bare Metal Recovery Kit** section.

Download the latest Windows ADK and Windows PE add-on for the ADK from [Microsoft](https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install) (<https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>).

← → ↻ <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>

Filter by title

Get started

- Download and install the Windows ADK**
- Install the ADK offline
- Kits and tools overview
- What's new in the Windows ADK and ADK tools
- What's new in Windows 10, version 1809

Download and install the Windows ADK

09/09/2018 • 2 minutes to read • Contributors 🧑🏫🧑🏫🧑🏫🧑🏫🧑🏫 all

The Windows Assessment and Deployment Kit (Windows ADK) has the tools you need to customize Windows images for large-scale deployment, and to test the quality and performance of your system, its added components, and the applications running on it. The Windows ADK includes:

- The Windows Assessment Toolkit and the Windows Performance Toolkit to assess the quality and performance of systems or components.
- Deployment tools such as WinPE, Sysprep, and other tools that you can use to customize and deploy Windows 10 images.
- Starting with Windows 10, version 1809, Windows Preinstallation Environment (PE) is released separately from the Assessment and Deployment Kit (ADK). To add Windows PE to your ADK installation, download the Windows PE Addon and run the included installer after installing the ADK. This change enables post-RTM updates to tools in the ADK. After you run the installer, the WinPE files will be in the same location as they were in previous ADK installs.

- [Download the Windows ADK for Windows 10, version 1809](#)
- [Download the Windows PE add-on for the ADK](#)
- [What's new in ADK tools for Windows 10, version 1809.](#)
- For Windows 10 IoT Core, also [download the IoT Core Add-Ins.](#)

Install the Windows ADK

1. Run **adksetup.exe** to install the Windows ADK.

 adksetup.exe	3/8/2019 1:32 PM	Application	1,857 KB
 adkwinpesetup.exe	3/8/2019 1:32 PM	Application	1,303 KB

2. Select **Install the Windows Assessment and Deployment Kit - Windows 10 to this computer** using the default **Install Path** . Click **Next**.
3. Specify whether you want to send your usage data to Microsoft. Click **Next**.
4. Click **Accept** to accept the license agreement.
5. Keep the default feature settings and click **Install**.
6. After the installation has completed successfully, uncheck the **Launch the Getting Started Guide** check box. Click **Close**.

Install the Windows PE Add-On for ADK

1. Run **adkwinsetup.exe** to install the Windows PE add-on for the ADK.

 adksetup.exe	3/8/2019 1:32 PM	Application	1,857 KB
 adkwinpesetup.exe	3/8/2019 1:32 PM	Application	1,303 KB

2. Select **Install the Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10 to this computer** using the default **Install Path** . Click **Next**.
3. Specify whether you want to send your usage data to Microsoft. Click **Next** .
4. Click **Accept** to accept the license agreement.

5. Keep the default feature settings and click **Install**.
6. After the installation has completed successfully, click **Close**.

Download and Extract the Barracuda Backup BMR Kit

1. Within Barracuda Backup, navigate to the **System > Software Downloads** page and download the **Barracuda Backup Bare Metal Recovery Kit**.
2. Unzip the **BarracudaBackupBmrKit-X.Y.ZZ.zip** archive file. Note the location of the extracted folder.
3. Open a command prompt and navigate to the BarracudaBackupBmrKit folder where you extracted the archive in Step 2.
4. Run the `create_bmr_iso.bat` script with the following commands that correspond to the ISO you want to create.
 - 64-bit ISO *without* additional drivers: `create_bmr_iso.bat amd64 C:\winpe-workspace C:\bmr.iso`
 - 64-bit ISO *with* additional drivers: `create_bmr_iso.bat amd64 C:\winpe-workspace C:\bmr.iso C:\drivers-for-bmr`
 - 32-bit ISO *without* additional drivers: `create_bmr_iso.bat x86 C:\winpe-workspace C:\bmr.iso`
 - 32-bit ISO *with* additional drivers: `create_bmr_iso.bat x86 C:\winpe-workspace C:\bmr.iso C:\drivers-for-bmr`Note that it will take several minutes for the script to build the BMR ISO.
5. Delete the directory you specified as the workspace (e.g. C:\winpe-workspace).

Prepare the Virtual Target

Before starting the restore, you must configure the system firmware option—BIOS or Extensible Firmware Interface (EFI)—on the target virtual system to match the original physical system (source). When you select a guest operating system, BIOS or EFI is selected by default, depending on the firmware supported by the operating system. If the operating system supports BIOS and EFI, you can change the default from the **Options** tab of the **Virtual Machine Properties** editor after you create the VM and before you install the guest operating system. If you select EFI, you cannot boot an operating system that supports only BIOS, and the reverse.

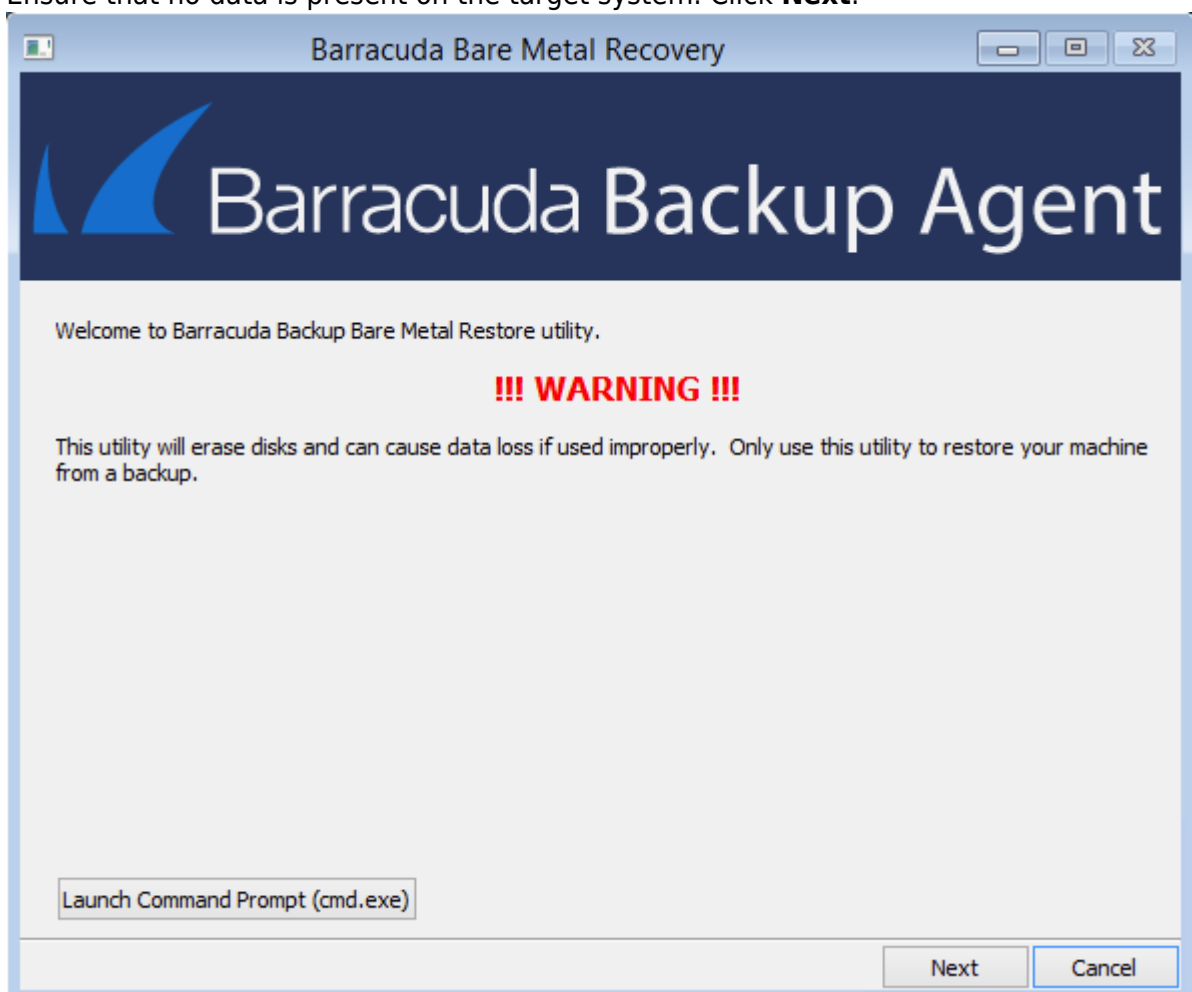
When creating the target VM in VMware or Hyper-V, use the same operating system architecture and configuration as the physical target system. For example, use the same CPU (x86 or x64), RAM, and disk configuration.

Perform Physical-to-Virtual Recovery

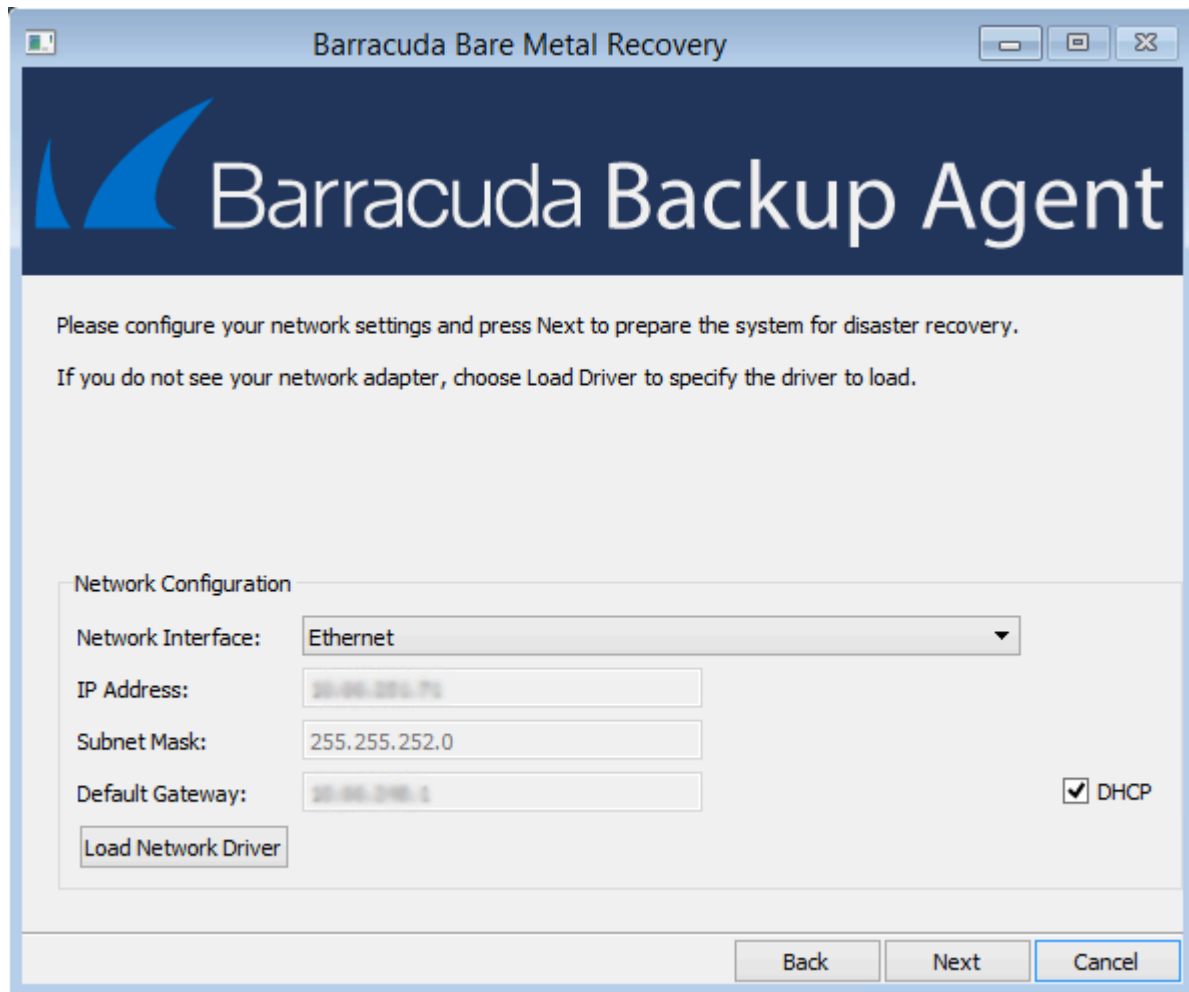
You must complete all of the steps described in the sections above, including downloading and installing Windows ADK and Windows PE add-on for ADK.

To perform a bare metal recovery:

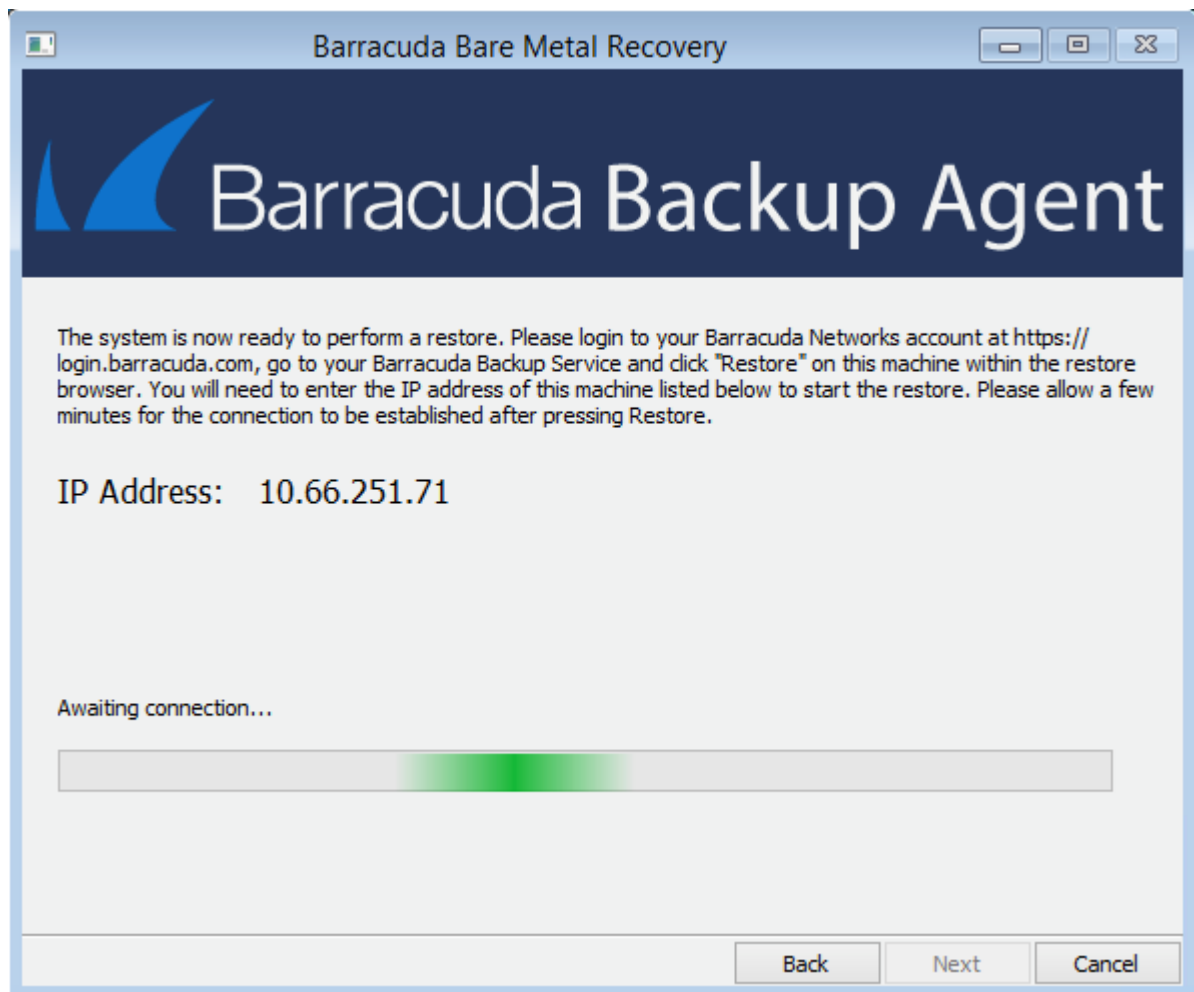
1. Use the Bare Metal Recovery ISO file you created above to boot the target system.
2. After the target system boots, the Bare Metal Restore Utility welcome/warning screen displays. Ensure that no data is present on the target system. Click **Next**.



3. On the **Network Configuration** screen, choose a **Network Interface**, and specify an **IP Address**, **Subnet Mask**, and **Default Gateway**. Then click **Next**.



4. The **Awaiting connection** screen displays.

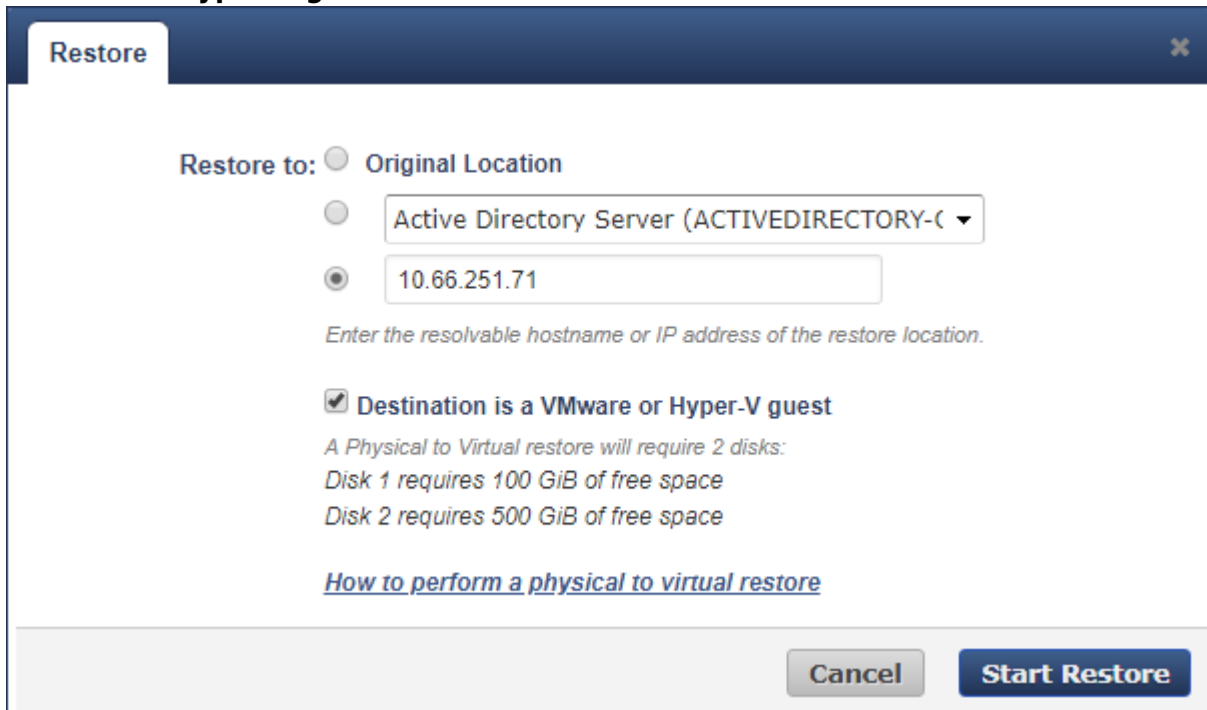


5. Log into the Barracuda Backup local or cloud interface, and go to the **Restore > Restore Browser** page.
6. Click **Restore** to the right of the Microsoft Windows system you want to restore. If you want to restore to a different backup revision of the system other than the latest, click on the system, and click **View all revisions up to: <date>**, and click **Restore** next to the backup revision.



7. In the **Restore** dialog box, select **Other Hostname or IP Address**, and type the IP Address

configured for the target system in the Bare Metal Restore Utility. Select **Destination is a VMware or Hyper-V guest**.



Restore

Restore to: Original Location

Active Directory Server (ACTIVEDIRECTORY-C...

10.66.251.71

Enter the resolvable hostname or IP address of the restore location.

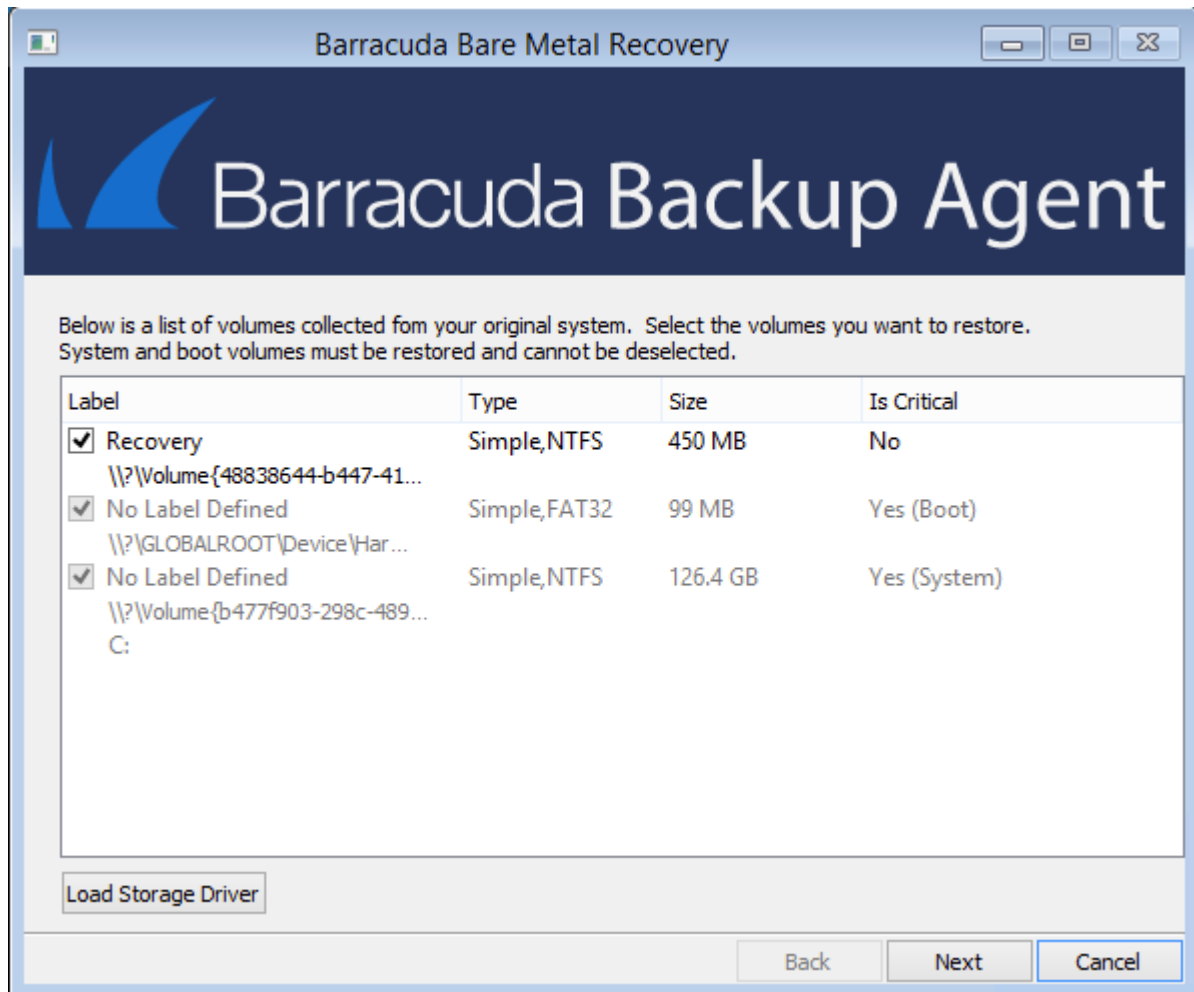
Destination is a VMware or Hyper-V guest

*A Physical to Virtual restore will require 2 disks:
Disk 1 requires 100 GiB of free space
Disk 2 requires 500 GiB of free space*

[How to perform a physical to virtual restore](#)

Cancel Start Restore

8. Click **Start Restore**.
9. After several minutes, the target system receives the restore job from Barracuda Backup and displays a list of recoverable volumes.

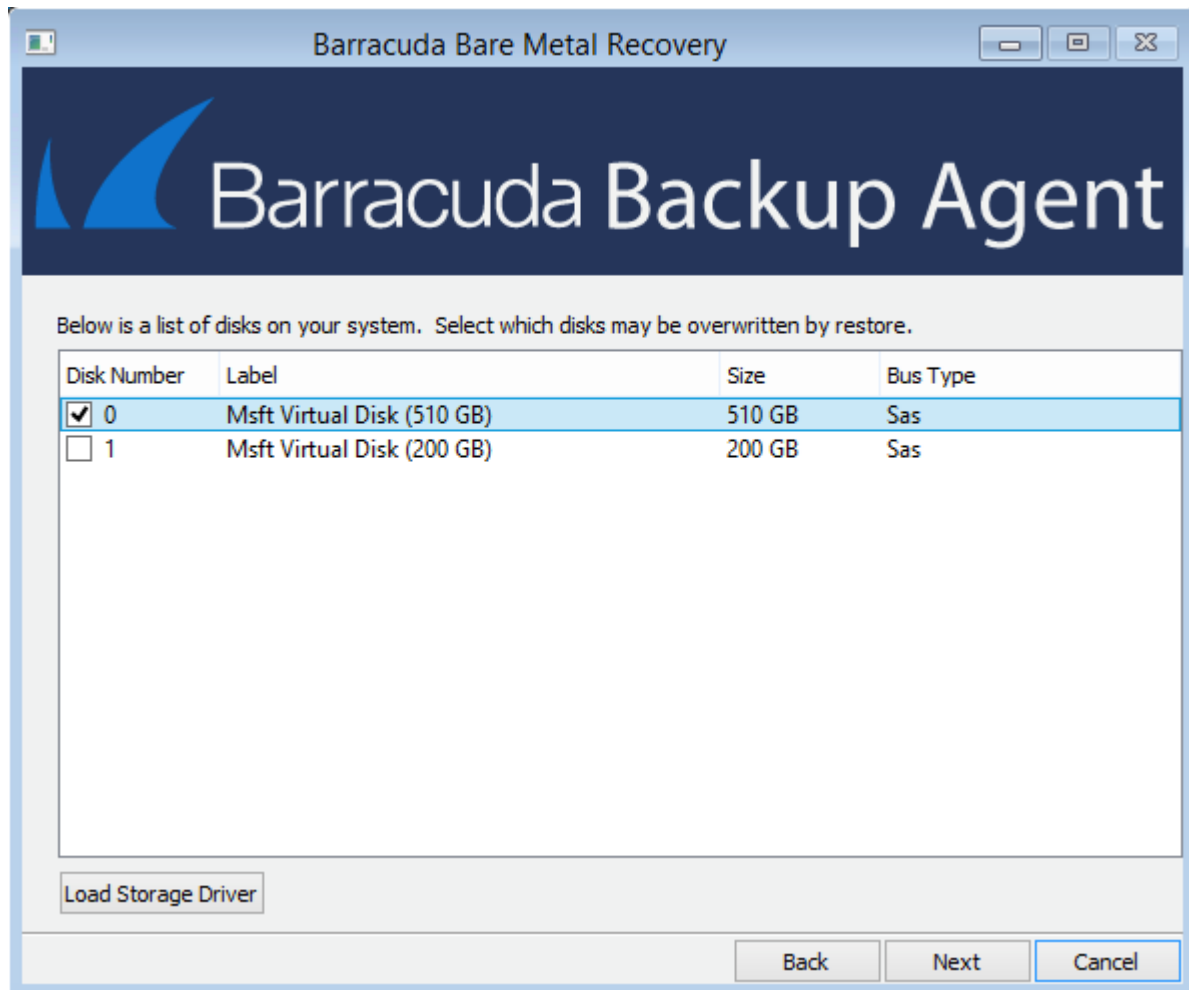


10. Select the volumes you want to recover. Click **Next**.

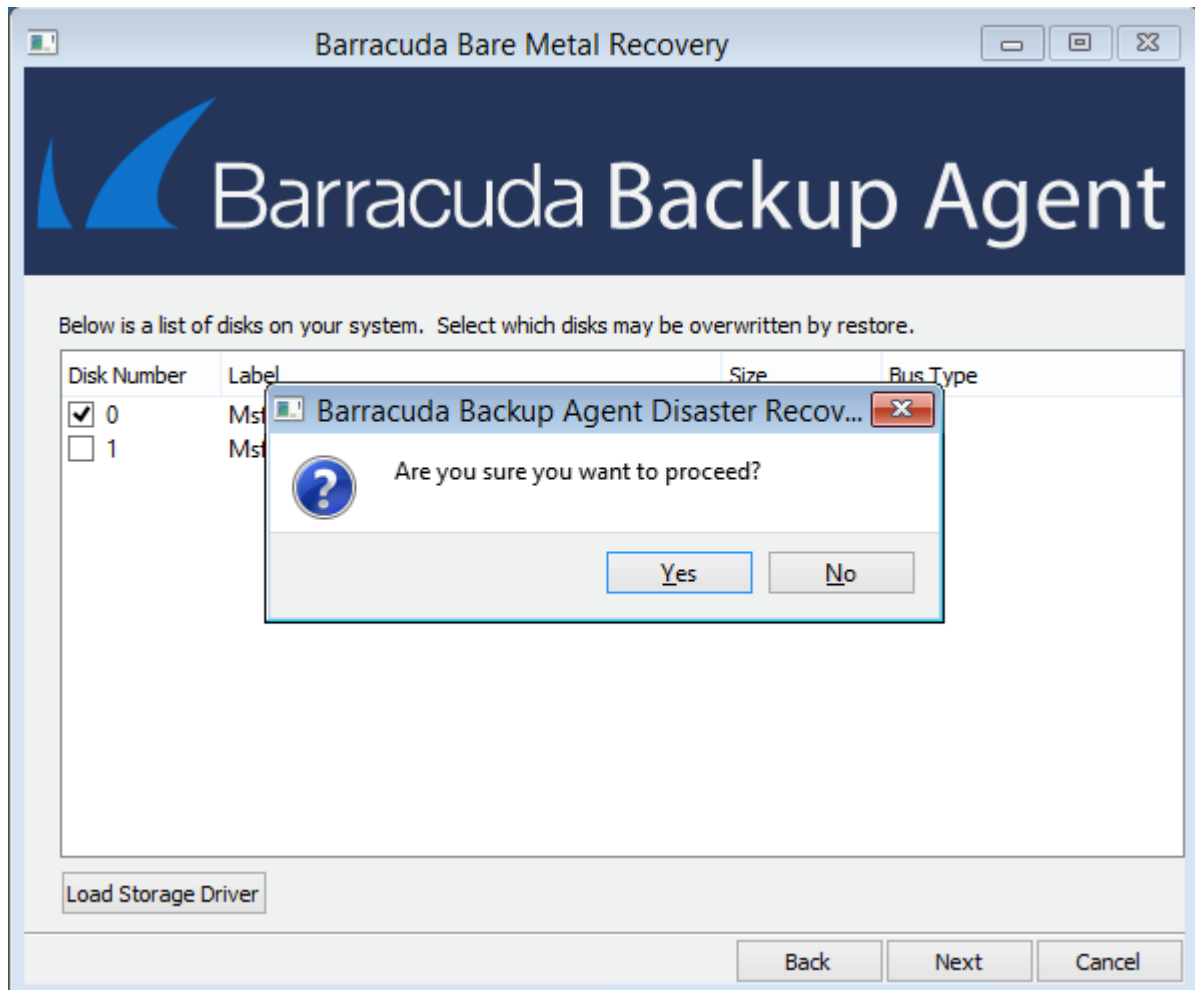
You cannot deselect boot and system volumes because they are required for the bare metal restore.

If you choose to restore to a server that does not have identical volumes as the original machine the data was backed up from, the Barracuda Backup appliance will still attempt to restore all drives even though you may have only selected one of these on the Bare Metal Restore screen. The restore will throw errors for these missing drives, but will restore the drives that exist on the target machine.

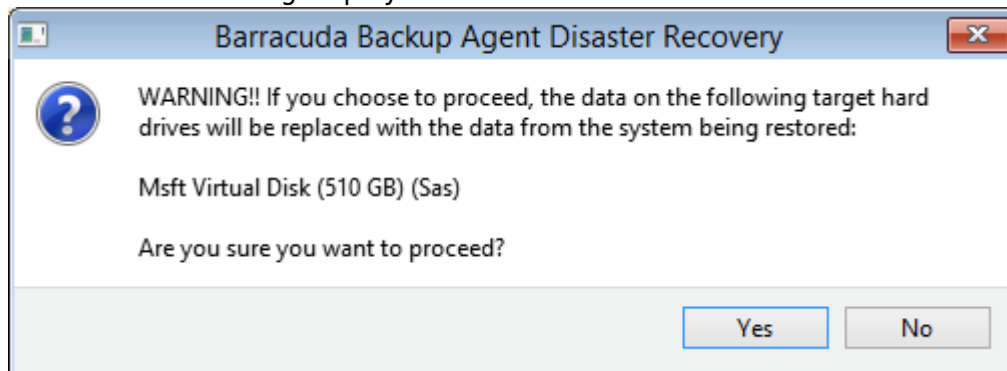
11. Select which disks on the target VM will be used in the recovery operation.



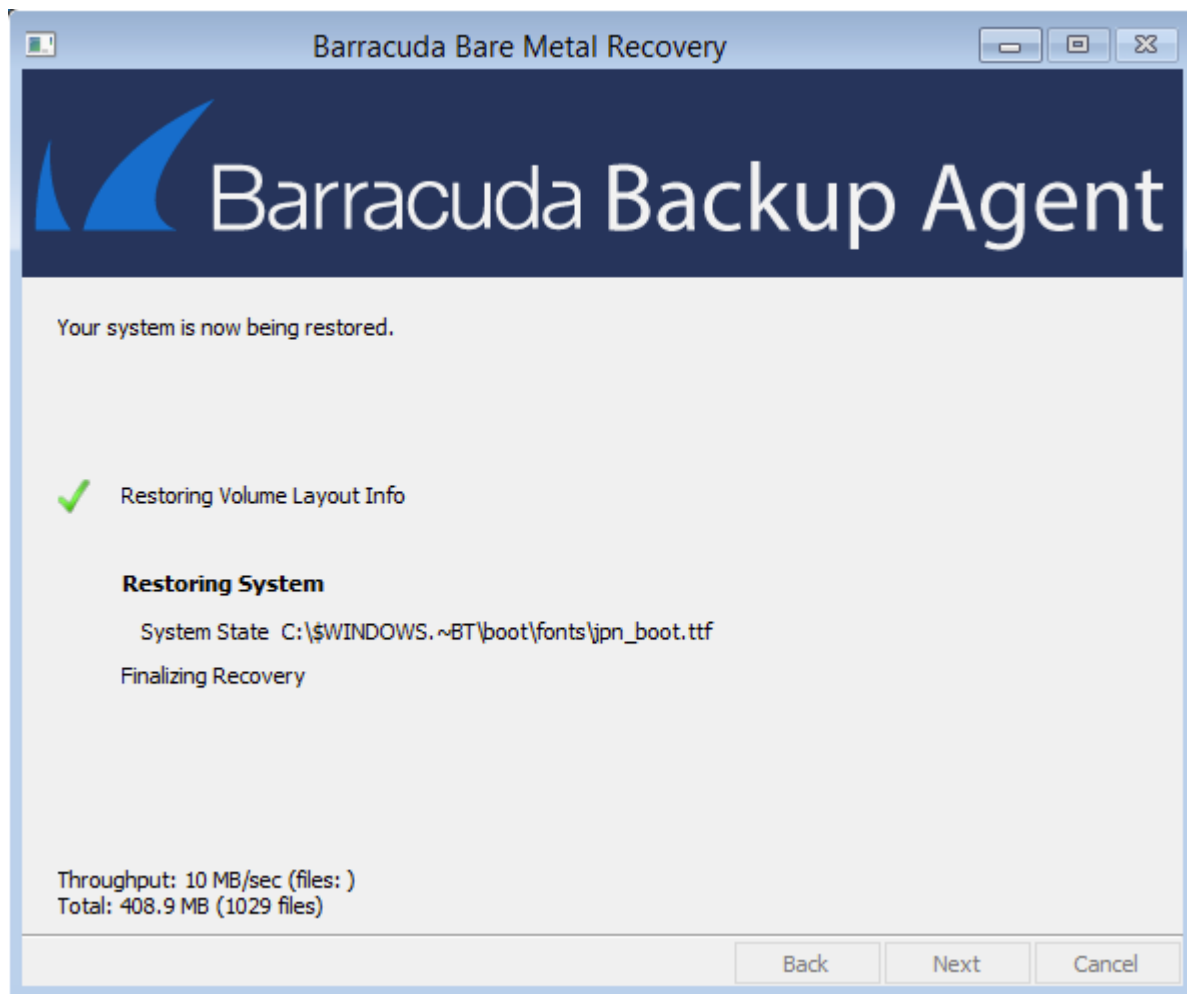
12. Click **Next**, then click **Yes** to confirm your selection.



13. An additional warning displays.



14. Click **Yes** to proceed. Click **Next** to begin the system restore.



15. When the restore is complete, click **OK** in the **Confirmation** dialog box.
16. Remove the Bare Metal Recovery ISO and reboot the system.

If the server being restored was an Exchange, SQL, or Hyper-V server, the application is installed after the bare metal restore. The databases or guest virtual machines (VMs) must be restored separately.

Figures

1. installadk.png
2. adksetup.png
3. adksetup.png
4. AgentWarning.png
5. Start.png
6. IP_Address.png
7. restore_link.png
8. Restore_VM.png
9. Select.png
10. BMR_new.png
11. ClickYes.png
12. warning.png
13. Confirm.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.