Bare Metal Protection and Recovery Guide

User Guide | December 2016

Bare Metal Protection and Recovery Guide

Release 9.1 | Document Version 1.12152016

unitrends.com

UNITRENDS

Copyright

Unitrends, Inc
200 Wheeler Road
North Tower, 2nd Floor

Burlington, MA 01803, USA
Phone: 1.866.359.5411

Contents

Chapter 1: Bare Metal Protection Overview

Bare metal technology is used for disaster recovery of the protected asset. Use the procedures in this guide to recover the assets protected by your Recovery Series or Unitrends Backup appliance. These procedures apply to the current user interface (UI). If you are using the legacy UI, see the bare metal procedures in the Administrator Guide for Recovery Series and Unitrends Backup - Legacy Interface instead. An overview of bare metal protection types is given here:

- Windows integrated bare metal – To protect many Windows assets, you can use their file-level backups and the integrated bare metal recovery ISO images provided on the Unitrends Recovery Series or Unitrends Backup appliance.
- Non-x86 platforms and Linux – To protect non-x86 platforms and Linux environments, burn a bare metal ISO image to CD and run periodic master backups. For disaster recovery, you boot from the CD, then restore the master backup followed by any differential and/or incremental backups.

Bare metal procedures by asset operating system

Asset operating system	**Bare metal procedures**
AIX	See "Bare metal for AIX" on page 53.
Hyper-V hypervisor	Protection is based on the operating system of the Hyper-V host. See the applicable procedure.
Hyper-V virtual machine	Protection is based on the operating system of the virtual machine. See the applicable procedure.
Linux	See "Bare Metal for Linux" on page 33.
Mac OS X	See "Bare metal for Mac OS X" on page 56.
Solaris (SPARC)	See "Bare Metal for Solaris SPARC" on page 59.

Asset operating system	Bare metal procedures
VMware virtual machine	Protection is based on the VM operating system. See the applicable procedure.
Windows XP, 2003, and up	See "Windows Hot Bare Metal Protection" on page 13.
Windows 2000	See "Windows Hot Bare Metal Protection" on page 13.

Considerations for bare metal test recovery

If you choose to perform a bare metal recovery as a test, there are several special conditions you need to be aware of:

- Network considerations - (These do not apply to integrated bare metal recovery. See "Performing a test integrated bare metal recovery" on page 32 instead.)

  When booting from a bare metal test CD, the asset will come on the network using the IP and hostname of the asset the CD was made for. When creating the bare metal boot disk for Windows assets, you have the option to manually change the IP and hostname when creating the disk. For all other asset operating systems, and for Windows assets whose bare metal boot disks' IPs and hostnames were not changed, it's critical that the test system not be connected to the same physical network if the original server is still online as this can cause an IP/DNS conflict.

  When you boot a server or virtual machine using a bare metal boot disk, the bare metal recovery software will look in the Unitrends system's host file to match an asset to its data. Therefore, when testing bare metal recovery it may be necessary to edit the asset's entry in the system's host file to a free IP address before booting from the bare metal media. See To view or edit the hosts file section under Networks for details on changing the IP.

  Note: Standard backup and recovery procedures for an asset whose host file entry you edit cannot occur until the entry is edited back.

- Active Directory considerations - Assets that are dependent on Active Directory for day to day functions may not function properly when recovered to a test network if a domain controller is not recovered into the test network first. If you plan to recover a domain controller with bare metals, it is extremely critical to perform this recovery into a test network.

Recovering aliased assets

When you perform disaster recovery of an asset with aliases, it’s important to recover them in a particular order.

Note: When you are backing up an aliased asset, you must decide whether to include or exclude the system state. You MUST include the system state on the asset that contains the operating system volumes (this is typically the C: volume). For all other asset aliases that do not include the OS volume, you should NOT include the system state. Only one asset alias can include the system state. The bare metal recovery fails if the system state is not included in the OS volume and if the system state is included in the asset aliases that do not include the OS volume. For more information, see Managing physical assets under the Managing protected assets section of the admin guide.

To perform bare metal recovery of an asset with aliases

1. First, recover the asset that contains the operating system and other critical volumes. You MUST do this before you recover any additional aliased assets. Follow the applicable procedure listed in "Bare metal procedures by asset operating system" on page 9 for details.
2. Next, recover each aliased asset. Follow the applicable procedure listed in "Bare metal procedures by asset operating system" on page 9 for details.

Chapter 2: Windows Hot Bare Metal Protection

Beginning in release 7.4, you have two options for hot bare metal recovery (BMR) of Windows assets: Windows integrated BMR and Windows image-based BMR (supported in Legacy UI only).

With Windows integrated BMR, Unitrends provides bare metal protection by enabling you to perform disaster recovery (DR) of your Windows asset right from its file-level backup. This reduces recovery time enabling you to meet more aggressive recovery time objectives (RTOs), provides additional recovery points enabling you to meet more aggressive recovery point objectives (RPOs), increases on-system retention by eliminating the need for bare metal backups, and simplifies the Windows DR process.

Windows DR is simplified with the new Integrated BMR Wizard and standard 32-bit and 64-bit ISO images that can be used to recover most Windows assets, eliminating the need to create bare metal ISOs for each protected asset and keep them on-hand in case disaster strikes.

Note: **About Windows virtual machines.** If you have Windows VMware or Hyper-V virtual machines, you can protect them using Unitrends VMware backups, Hyper-V backups, or by installing the Windows agent and running Unitrends file-level backups. If you are running agent-based file-level backups for a VM, use the hot bare metal procedures in this chapter for Disaster Recovery. If you are running VMware or Hyper-V backups for a VM, restore the virtual machine using the procedures found in Recovering a virtual machine.

For details, see the following topics:

- "Windows integrated bare metal recovery" on page 13
- "Implementing Windows integrated bare metal protection" on page 14

Windows integrated bare metal recovery

With the Windows integrated bare metal recovery feature (release 7.4 or higher), you can protect a Windows asset’s operating system without having to run bare metal backups or create ISO images for each of your Windows assets. File-level backups run with agent version 7.4 or higher capture the disk metadata necessary for the recovery, and backup systems running release 7.4 or higher contain standard 32-bit and 64-bit ISO images that you can use for the recovery. You can recover an asset from eligible file-level backups residing on a Unitrends backup system or replication target running release 7.4 or higher. The destination for the recovery can be a physical or virtual machine.

When you boot the destination machine from the standard ISO, it boots into WinPE 4, a minimal version of Windows used for installations, and the Windows Integrated Bare Metal Recovery Wizard launches to guide you through the recovery. Depending on your operating system and hardware, it might be necessary to add drivers to WinPE and the restored operating system during the recovery. You can use the wizard interface to add drivers.

With integrated BMR, you can restore only critical volumes, so to complete the recovery, you will need to perform file-level recovery to restore files that reside on non-critical volumes. After restoring the critical volumes, injecting any necessary drivers, and configuring network settings on the new machine, you can connect to the Unitrends backup system to restore your files. If, however, all of your data resides on the critical volumes, it is restored through the integrated BMR and the recovery of your failed asset is complete.

See the following topics for details about protecting the operating systems of your Windows assets using the integrated bare metal recovery feature:

- "Implementing Windows integrated bare metal protection" on page 14
- "Prerequisites for Windows integrated bare metal recovery" on page 15
- "Supported integrated bare metal recovery scenarios" on page 16
- "About eligible backups for Windows integrated bare metal recovery" on page 17
- "About integrated bare metal recovery ISO images" on page 18
- "About adding drivers during the integrated bare metal recovery" on page 18
- "Performing the integrated bare metal recovery" on page 19
- "Performing a test integrated bare metal recovery" on page 32

Implementing Windows integrated bare metal protection

For best results, it is recommended that you plan your strategy for disaster recovery before an asset fails. This section provides a high-level overview of the steps you must complete to implement integrated bare metal protection for your Windows assets. It identifies steps to complete before and after an asset fails.

Perform the following before an asset fails

Step 1: Determine which Windows operating system the asset is running and whether it is the 32-bit or 64-bit version. For instructions, see the Microsoft document Which Windows operating system am I running?

Step 2: Verify that the asset's operating system is supported, and review the additional considerations for integrated BMR. See "Prerequisites for Windows integrated bare metal recovery" on page 15.

Step 3: Determine whether the asset's firmware interface type is BIOS or UEFI. In most version of Windows, you can determine the firmware interface type by viewing system information (as described in the Microsoft document What is System Information?) or by viewing the Windows machine's volumes in the computer management tool (see the Microsoft document What are Administrative Tools?).

Step 4: Upgrade your backup system to release 7.4 or higher. For instructions on updating your system, see Managing appliances .

Step 5: Install Windows agent version 7.4 or higher. See Installing the Windows agent versions for details about Windows agents.

Step 6: Run file-level backups that include disk metadata. Disk metadata is captured in all file-level backups run with agent version 7.4 or higher unless you exclude critical volumes using selection lists. (For details about running file-level backups, see Creating backup jobs .

Step 7: Review the recovery scenarios described in "Supported integrated bare metal recovery scenarios" on page 16.

To recover a failed asset

Step 8: Perform the integrated BMR recovery using the procedures described in "Performing the integrated bare metal recovery" on page 19.

Prerequisites for Windows integrated bare metal recovery

Consider the prerequisites for integrated BMR as you plan your disaster recovery strategy.

Supported operating systems

Recovery to identical hardware and virtual machines is supported for the operating systems listed below.

- Windows XP (32-bit and 64-bit)
- Windows Server 2003 (32-bit and 64-bit)
- Windows Server 2003 R2 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)

- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)

Recovery to dissimilar hardware is supported for assets running Windows Vista/Server 2008 and later.

Additional considerations for integrated BMR

- GPT disks are supported.
- Dynamic disks are not supported.
- BIOS- and UEFI-based assets are supported. The firmware interface type (BIOS or UEFI) of the destination machine must match that of the failed assett.
- Backups used for the recovery must contain disk metadata (For details, see "About eligible backups for Windows integrated bare metal recovery" on page 17.)
- Backups used for the recovery must have been run with agent version 7.4 or higher.
- Recovery to a virtual machine is supported on VMware ESX/ESXi 5.0 and higher and all versions of Hyper-V.
- Wireless network adapters cannot be used for the recovery.
- The integrated bare metal recovery ISO image contains WinPE 4.0, which is based on Windows 8. If you are restoring to a physical machine, you might need to add Windows 8 drivers for the restore. For more about adding drivers during the recovery process, see "About adding drivers during the integrated bare metal recovery" on page 18.
- WinPE 4.0 requires the processor features NX, PAE, SSE2 to be enabled. You might need to enable these features for a physical destination machine before booting from the ISO image. For instructions, see KB 1190. Machines that do not have these processor features cannot be used for the restore.
- After recovering a Hyper-V server, you must run the following command on the Hyper-V server: *bcdedit /set hypervisorlaunchtype Auto*. You should then reboot the server.

Supported integrated bare metal recovery scenarios

The supported integrated bare metal recovery scenarios are listed below. You can perform all of the recovery scenarios using the instructions provided in "Performing the integrated bare metal recovery" on page 19.

- Restore to same physical hardware as the failed asset. Supported for all operating systems listed in "Prerequisites for Windows integrated bare metal recovery" on page 15.
- Restore a failed physical asset to a virtual machine (Hyper-V/VMware). Supported for all operating systems listed in "Prerequisites for Windows integrated bare metal recovery" on page 15. Supported on VMware ESX/ESXi 5.0 and higher and all versions of Hyper-V.
- Restore a failed virtual asset to a virtual machine. Supported for all operating systems listed in "Prerequisites for Windows integrated bare metal recovery" on page 15. Supported on VMware ESX/ESXi 5.0 and higher and all versions of Hyper-V.
- Restore a failed virtual client to a physical machine. Supported for Windows 7/ Server 2008 R2 and higher.

Note: To restore a failed virtual asset using the integrated bare metal recovery feature, you must have protected the client using agent backups. If you have protected the asset with VM backups, you can use the procedures for restoring an entire VM from a backup. For details, see Recovering a virtual machine.

- Restore a failed physical asset to dissimilar hardware. Supported for Windows Vista/Server 2008 and higher.
- Restore a failed physical asset to dissimilar hardware with fewer disks. Supported for Windows Vista/Server 2008 and higher.
- Restore a failed physical asset to hardware with smaller or larger disks. Supported for all operating systems listed in "Prerequisites for Windows integrated bare metal recovery" on page 15.
- Restore a failed asset BIOS/MBR configuration to dissimilar BIOS/MBR configuration. Supported for Windows Vista/Server 2008 and higher.
- Restore a failed asset UEFI/GPT configuration to dissimilar UEFI/GPT configuration. Supported for Windows Vista/Server 2008 and higher.
- Restore multi-boot configured BIOS servers.

About eligible backups for Windows integrated bare metal recovery

For an asset’s operating system to be recovered using the integrated BMR feature, eligible file-level backups for the asset must reside on a Unitrends Recovery Series or Unitrends Backup appliance or backup copy target running release 7.4 or higher. A file-level backup is eligible for an integrated BMR if it meets all of the following criteria:

- It is successful.
- It is a full, differential, or incremental file-level backup that contains disk metadata. Disk metadata is captured in all file-level backups run with agent version 7.4 or higher unless

you exclude critical volumes using selection lists. If you are using selection lists, and you want to determine whether a backup is eligible, see "To verify that a file-level backup is eligible for integrated bare metal recovery" on page 18.

- It was run with agent version 7.4 or higher.

Note: Bare metal backups cannot be used for integrated bare metal recovery. You can recover an operating system from a bare metal backup using the procedure described in Windows image-based bare metal recovery. However, if you have eligible file-level backups for a failed asset, it is recommended that you use one of these backups to perform an integrated bare metal recovery to take advantage of significant performance enhancements.

To verify that a file-level backup is eligible for integrated bare metal recovery

1. View backup details by going to the Jobs page and clicking on the Recent Jobs tab and finding the desired backup. Click the View Log to see if the system state was included in the backup.
2. Verify that for System State, the Entry is *Included.*

   If the Entry is *Included,* then the backup contains disk metadata, and it is eligible for integrated BMR. If the Entry is *Excluded*, then the backup does not contain disk metadata, and it is not eligible.
3. Repeat step 2 on page 18 as needed to determine whether other backups are eligible. If no eligible backups reside on your backup system, then you must run new file-level backups that capture disk metadata if you want to use integrated BMR in the event that the asset fails. For details see Creating backup jobs.

About integrated bare metal recovery ISO images

For the recovery, you must use the 32-bit or 64-bit integrated BMR ISO image provided on the Recovery Series or Unitrends Backup appliance. The ISO contains WinPE 4.0, a minimal version of Windows used for installations, and the Unitrends Integrated Bare Metal Recovery Wizard that guides you through the recovery. For details about WinPE 4.0, see the Microsoft TechNet document WinPE: Windows PE Overview. To access the images, see "Accessing the integrated bare metal recovery ISO images" on page 20.

About adding drivers during the integrated bare metal recovery

Depending on the recovery destination and your operating system, you might need to add drivers during different stages of the recovery. For details, see the following topics:

- "Loading WinPE drivers for integrated bare metal recovery" on page 19
- "Injecting restored operating system drivers for integrated bare metal recovery" on page 19

Loading WinPE drivers for integrated bare metal recovery

The Integrated BMR Wizard uses WinPE 4.0 for the recovery. WinPE 4.0 is based on Windows 8, and if it cannot detect a network adapter or storage disks, you must load Windows 8 drivers into WinPE for the restore.

Note: WinPE 4.0 is used only for the restore. After the wizard restores the critical volumes from the failed asset, you might need to inject additional drivers into the restored operating system before you can reboot the restored asset.

Injecting restored operating system drivers for integrated bare metal recovery

After the critical volumes have been restored, you must inject drivers into the restored operating system if you are restoring to dissimilar hardware or to a virtual machine. If you restore to a physical machine, drivers vary depending upon the hardware and operating system. It is recommended that you verify whether the operating system requires additional drivers to run on the hardware to which you will restore before beginning the recovery. If you restore to a virtual machine, you must inject ESX or Hyper-V guest storage drivers, depending upon your virtual environment. These drivers are included in the integrated BMR ISO image.

Performing the integrated bare metal recovery

This section provides a high-level overview of the steps you must complete to perform the integrated bare metal recovery. Before beginning the recovery, it is recommended that you read "Implementing Windows integrated bare metal protection" on page 14, which provides an overview of the recovery process and identifies the prerequisites and supported recovery scenarios. You can perform all of the recovery scenarios using the Integrated Bare Metal Recovery Wizard, as described in "Running the integrated Bare Metal Recovery Wizard" on page 22.

Use the following steps to perform the recovery:

Step 1: "Accessing the integrated bare metal recovery ISO images" on page 20

Step 2: "Preparing the destination machine for an integrated bare metal recovery" on page 20

Step 3: "Running the integrated Bare Metal Recovery Wizard" on page 22

Step 4: "Post-restore driver injection" on page 30

Note: This step is required only when restoring to dissimilar hardware.

Step 5: "Completing the integrated bare metal recovery" on page 31

Accessing the integrated bare metal recovery ISO images

For the recovery, you must use the 32-bit or 64-bit integrated BMR ISO image provided on the Recovery Series or Unitrends Backup appliance. The ISO contains WinPE 4.0, a minimal version of Windows used for installations, and the Unitrends Integrated Bare Metal Recovery Wizard that guides you through the recovery. Use the procedure described below to access the 32-bit and 64-bit ISO images.

To access the integrated bare metal recovery ISO images

1. Mount a working asset to the Samba share *virtual_failover* on your Unitrends appliance.

   Mounting procedures vary depending upon the operating system, but for most Windows versions, you should be able to access the Map network drive option after selecting Computer. For example, to mount to the *virtual_failover* share in Windows 7, you can select Computer and then Map network drive. You can then map to the Samba share by entering the following in the Folder field: \\<*IP address of your Unitrends appliance*>*virtual_failover*.
2. Select *winbm32* for 32-bit BIOS-based assets and *winbm* for 64-bit BIOS-based assets. Select *winbm* for 32-bit and 64-bit UEFI assets.
3. Burn the image to a disk for recovery to a physical machine, or save it in a location that you can access from your hypervisor for recovery to a virtual machine.
4. Proceed to "Preparing the destination machine for an integrated bare metal recovery" on page 20 to continue the recovery.

Preparing the destination machine for an integrated bare metal recovery

You can restore a failed asset to a physical or virtual machine. Your first step in performing the integrated bare metal recovery is to prepare the destination machine.

See the topics below for instructions:

- "To prepare a physical machine for an integrated bare metal recovery" on page 20
- "To prepare a virtual machine for an integrated bare metal recovery" on page 21

To prepare a physical machine for an integrated bare metal recovery

Note: WinPE 4.0 requires the processor features NX, PAE, SSE2 to be enabled. You might need to enable these features for the destination machine before booting from the ISO image. For instructions, see KB 1190. Machines that do not have these processor features cannot be used for the restore.

1. Determine whether the machine's firmware interface type (BIOS or UEFI) matches the firmware interface type of the failed asset.

   If you do not know whether the failed asset's firmware interface type is BIOS or UEFI, you can attempt the recovery, but the restored asset will not boot if you try to restore to a dissimilar interface type.

2 Make sure the machine has enough disk space for the recovery.

- The recovery destination can have smaller disks than the failed asset; however, if the disks on the target machine do not have enough space for the data on the critical volumes, the restore will fail.

Note: After an asset has failed, there is no way to determine the size of its critical volumes. You can determine the size of an asset's backup by viewing the backup details in the Backup History report on the Reports page. However, the size of the critical volumes will be smaller than the total size of a full backup if it also contains non-critical volumes. If you are unsure about the size of the critical volumes, it is recommended that you recover the failed asset to destination disks that are the same size as the original disks or larger.

CAUTION! If you are recovering to new disks, any existing data on the destination disks is overwritten or deleted during the restore, even if the disks have more than enough space. Before performing a recovery, make sure you have additional copies of any data on the destination disks. If you are recovering to the original disk, only the restored volumes are overwritten. Other volumes on the original disk are not impacted by the restore.

3 Load the disk with the burned ISO image into the machine's CD/DVD drive. For instructions on accessing the ISO, see "Accessing the integrated bare metal recovery ISO images" on page 20.

4 Proceed to "Running the integrated Bare Metal Recovery Wizard" on page 22 to begin the integrated bare metal recovery.

To prepare a virtual machine for an integrated bare metal recovery

1 Create a Hyper-V or VMware virtual machine or edit the settings of an existing VM.

- Make sure the VM's firmware interface type (BIOS or UEFI) matches the firmware interface type of the failed asset.
- Add enough memory to satisfy Microsoft's support guidelines for the operating system being recovered. The integrated bare metal recovery ISO requires at least 1 GB of memory.

- Assign the VM a virtual hard disk with enough memory for the recover. You can recover to a disk that is smaller than the original disk, but the restore fails if the disk does not have enough space for the critical volumes.

Note: After an asset has failed, there is no way to determine the size of its critical volumes. You can determine the size of an asset’s backup by viewing the backup details in the Backup History report on the Reports page. However, the size of the critical volumes will be smaller than the total size of a full backup if it also contains non-critical volumes. If you are unsure about the size of the critical volumes, it is recommended that you restore the failed asset to destination disks that are the same size as the original disks or larger.

CAUTION! If you are recovering to new disks, any existing data on the destination disks is overwritten or deleted during the restore, even if the disks have more than enough space. Before performing a restore, make sure you have additional copies of any data on the destination disks. If you are recovering to the original disk, only the restored volumes are overwritten. Other volumes on the original disk are not impacted by the restore.

- For a VMware virtual machine, make sure you are using the E1000 NIC.

Note: This requirement is necessary only for the restore. After rebooting the restored asset, you can use a different NIC.

- Add the bare metal ISO image to the VM’s disk drive. For instructions on accessing the ISO, see "Accessing the integrated bare metal recovery ISO images" on page 20.

2 Proceed to "Running the integrated Bare Metal Recovery Wizard" on page 22 to begin the integrated bare metal recovery.

Running the integrated Bare Metal Recovery Wizard

Perform the recovery process using the Integrated Bare Metal Recovery Wizard. See the following topics for details:

- "To perform the integrated bare metal recovery to a physical destination" on page 22
- "To perform the integrated bare metal recovery to a virtual destination" on page 26

To perform the integrated bare metal recovery to a physical destination

Follow these instructions to restore to identical or dissimilar hardware.

Note: If you exit the Integrated BMR Wizard before you are finished with the recovery, you are taken to a command window. To return to the wizard from this window, run the following command: z:\pcpb\Restore.exe.

1 Prepare the destination machine using the procedure described in "Preparing the destination machine for an integrated bare metal recovery" on page 20.

2 Boot the destination machine from the bare metal ISO image. The machine boots in WinPE 4, and the first screen of the Integrated Bare Metal Recovery Wizard displays.

> **Note:** If a message displays stating that you must set up networking to continue or that no disks are detected on the local system, you might need to load drivers into WinPE. Click ***Ok*** to allow the boot to continue. If necessary, you can load drivers as part of the next step.

To set up the local environment for the integrated bare metal recovery

To begin the recovery process, you must set up the local environment to ensure that the destination machine can communicate with the appliance that is storing the backup you will use for the recovery.

3 Select a network adapter in the drop-down menu to begin configuring network settings for the destination machine. If the machine has more than one adapter, the default adapter displays first.

If a network adapter does not display, WinPE cannot detect one. To resolve this problem, perform the following:

- Ensure that the network cable is plugged in to an active port.
- If the adapter is connected to the network and WinPE is unable to detect it, you must load a Windows 8 network driver into WinPE. Use the Load WinPE Drivers section of the wizard screen to enter a Path for a driver or Browse to locate a driver.

4 Skip this step unless the wizard informs you that no disks are detected on the local systems. If no disks are detected, you must load Windows 8 storage drivers into WinPE. Use the Load WinPE Drivers section of the wizard screen to enter a Pathfor a driver or Browse to locate a driver.

5 If DHCP is configured for your network, network settings are assigned automatically. If DHCP is not configured, or if you wish to configure network settings for the target machine manually, click **Change Settings**. Then enter a unique IP address for the machine, and the Subnet Mask and the Gateway for the network. It is not necessary for the network settings to match those of the original asset. The only requirement for network setup is that the machine can communicate with the appliance that is storing the backup that you will use for the recovery.

> **Note:** The network settings that you configure during this step are used only for the restore. They are not applied to the network adapter when you reboot the restored operating system. Before connecting the restored asset to your network, you must reconfigure the asset's network settings.

6. Select the time zone of the Unitrends system storing the backup that you will use for the restore.
7. Click **Next** to proceed to the next screen in the wizard.

To select a source and recovery point for integrated bare metal recovery

You must now select an appliance and recovery point for the restore.

8. Select a source for the restore. The wizard detects any backup systems and replication targets on the same subnet as the destination machine and displays them in the Backup Source drop-down menu. Select a system from this drop-down menu, or enter the IP address for a different system if you want to restore from a system on a different subnet.

   If you are using replication, when selecting the source for the restore, you must determine whether you want to restore from a asset's local or replicated backup. To restore from a local backup, you must select a backup system containing local backups for the asset. To restore from a replicated backup, you must select the target to which the asset's backups have replicated.
9. Select an Asset from the drop-down menu. Only assets with eligible backups display in the menu. Eligible backups contain the system state data necessary for the integrated bare metal recovery. For more about eligible backups, see "About eligible backups for Windows integrated bare metal recovery" on page 17.
10. Select a recovery point in the calendar. If multiple backups exist for an asset on a given day, the different times for these backups display in the Recovery Point drop-down menu. If the recovery times do not match the backup times on the Unitrends system, verify that in step 6 on page 24 you selected the time zone of the system that you are using for the restore.

    Click **Next** to continue.

To map drives/volumes for integrated bare metal recovery

After selecting an appliance, asset, and recovery point for the restore, you must map the failed asset's disks and volumes to disks in the recovery destination.

11. In the Drive/Volume Mapping screen of the Integrated Bare Metal Recovery Wizard, select critical volumes from the asset's backup to restore to the destination machine.

    - Disks and critical volumes (boot, system, and other critical volumes) that can be restored from the recovery point you have selected display in the Source Disks/Volumes window in the top part of the screen. GPT disks are identified in the window. For the most recent versions of Windows, two volumes display: a boot volume and a system volume. For most older versions, the boot and system files are on a single volume. Some assets require additional critical volumes to boot, and these volumes also display in the Drive/Volume Mapping screen.

- Non-critical volumes do not display because they cannot be restored through the Integrated Bare Metal Recovery Wizard. (For details about restoring non-critical volumes after performing the bare metal recovery, see "Completing the integrated bare metal recovery" on page 31.)
- If the recovery destination is reasonably similar to the original machine, the wizard automatically maps the backed up volumes to the destination disk. To perform the mapping manually, uncheck the box next to Restore to original system (automatic mapping).
- The wizard does not require you to select all critical volumes displayed in the Source Disks/Volumes window to proceed, but for the recovery to succeed, you must select the volumes necessary for the operating system to boot. If you are unsure, select all critical volumes displayed in the window. You can select all critical volumes by highlighting the disk that contains them.

12 Add selected volumes to the Destination Disks window in the bottom half of the integrated BMR screen.

After highlighting the necessary volumes in the Source Disks/Volumes window, highlight the destination disk in the Destination Disks window. Then click **Add** to map the volume to the destination disk. To remove a volume, select the volume you wish to remove and click **Remove**.

Consider the following when selecting a destination disk for the restore:

- If you are restoring to a new disk, and this destination contains existing volumes, they are deleted during the restore and new volumes are created. If you are restoring to the original disks, only the restored volumes are overwritten. Other volumes on the original disk are not impacted by the restore.
- It is recommended that the destination disk be the same size as the original disk or larger to ensure that there is enough space for the critical volumes. However, the destination disk can be smaller than the original disk. Before initiating the recovery, you must make sure that the disk is large enough for the critical volumes; otherwise, the recovery will run until the disk is full, and then it will fail.

Note: The disk/volume sizes displayed in the Source Disk/Volume window are the total capacity of the original disks/volumes and not the size of the backup that will be restored. After an asset has failed, there is no way to determine the size of its critical volumes. You can determine the size of an asset’s backup by viewing the backup details in the Backup History report on the Reports page. However, the size of the critical volumes will be smaller than the total size of a full backup if it also contains non-critical volumes. If you are unsure about the size of the backed up data on the critical volumes, it is recommended that you restore the failed asset to destination disks that are the same size as the original disks or larger.

- Volumes are assigned numbers during the restore that do not necessarily match the numbers from the original disk.
- For dissimilar restores of multi-boot configured BIOS servers, the boot and system volumes must be restored to the same disk numbers used on the original server.

Click **Next** to proceed to the Execute the Restore screen.

To execute the integrated BMR

13 Click **Restore** in the Execute the Restore screen to start the restore.

The Integrated BMR Wizard assigns the restore a job number. You can monitor its progress in the Restore Progress window in the top half of the wizard screen or in the Status screen of the appliance where the backed up volumes reside.

The restore process can take several minutes.

14 If the restore destination has hardware that is identical to that of the failed asset, you are ready to reboot the destination machine. Click **Reboot**, and then proceed to step 15.

If you have restored to dissimilar hardware, you must inject drivers before rebooting. Skip to "Post-restore driver injection" on page 30.

15 When the restored asset reboots, proceed to "Completing the integrated bare metal recovery" on page 31.

Note: If the restored asset fails to boot, you might need to inject drivers. To inject drivers, boot the machine from the disk and follow the instructions described in "Post-restore driver injection" on page 30.

To perform the integrated bare metal recovery to a virtual destination

Note: If you exit the Integrated BMR Wizard before you are finished with the recovery, you are taken to a command window. To return to the wizard from this window, run the following command: z:\pcpb\Restore.exe.

1 Prepare the destination machine using the procedure described in "Preparing the destination machine for an integrated bare metal recovery" on page 20.

2 Boot the destination virtual machine from the integrated bare metal ISO image. The machine boots in WinPE 4, and the first screen of the Integrated Bare Metal Recovery Wizard displays.

To set up the local environment for integrated bare metal recovery

To begin the recovery process, you must set up the local environment to ensure that the destination machine can communicate with the appliance that is storing the backup that you will use for the recovery.

3 Select a network adapter in the drop-down menu to begin configuring network settings for the destination machine. If the machine has more than one adapter, the default adapter displays first.

4 If DHCP is configured for the VM's host, network settings are assigned automatically. If DHCP is not configured, or if you wish to configure network settings for the target VM manually, click **Change Settings**. Then enter a unique IP address for the VM, and the Subnet Mask and the Gateway for the network. It is not necessary for the network settings to match those of the original asset. The only requirement for network setup is that the VM can communicate with the appliance that is storing the backup that you will use for the recovery.

> **Note:** The network settings that you configure during this step are used only for the restore. They are not applied to the network adapter when you reboot the restored operating system. Before connecting the restored asset to your network, you must reconfigure the asset's network settings.

5 Select the time zone of the Unitrends system storing the backup that you will use for the restore.

6 Click **Next** to proceed to the next screen in the wizard.

To select a source and recovery point for integrated bare metal recovery

You must now select an appliance and recovery point for the restore.

7 Select a source for the restore. The wizard detects any backup systems and replication targets on the same subnet as the VM and displays them in the Backup Source drop-down menu. Select a system from this drop-down menu, or enter the IP address for a different system if you want to restore from a system on a different subnet.

If you are using replication, when selecting the source for the restore, you must determine whether you want to restore from an asset's local or replicated backup. To restore from a local backup, you must select a backup system containing local backups for the asset. To restore from a replicated backup, you must select the target to which the asset's backups have replicated.

8 Select an Asset from the drop-down menu. Only assets with eligible backups display in the menu. Eligible backups contain the system state data necessary for the integrated bare metal recovery. For more about eligible backups, see "About eligible backups for Windows integrated bare metal recovery" on page 17.

9 Select a recovery point in the calendar. If multiple backups exist for an asset on a given day, the different times for these backups display in the Recovery Point drop-down menu. If the recovery times do not match the backup times on the Unitrends system, verify that in Step 5 you selected the time zone of the system that you are using for the restore.

Click **Next** to continue.

To map drives/volumes for integrated bare metal recovery

After selecting an appliance, asset, and recovery point for the restore, you must map the failed asset’s disks and volumes to disks in the recovery destination.

10 In the Drive/Volume Mapping screen of the Integrated Bare Metal Recovery Wizard, select critical volumes from the asset’s backup to restore to the destination machine.

- Disks and critical volumes (boot, system, and other critical volumes) that can be restored from the recovery point you have selected display in the Source Disks/Volumes window in the top part of the screen. GPT disks are identified in the window. For the most recent versions of Windows, two critical volumes display: a boot volume and a system a volume. For most older versions, the boot and system files are on a single volume. Some assets require additional critical volumes to boot, and these volumes also display in the Drive/Volume Mapping screen.
- Non-critical volumes do not display because they cannot be restored through the Integrated Bare Metal Recovery Wizard. (For details about restoring non-critical volumes after performing the bare metal recovery, see "Completing the integrated bare metal recovery" on page 31.)
- If the recovery destination is reasonably similar to the original machine, the wizard automatically maps the backed up volumes to the destination disk. To perform the mapping manually, uncheck the box next to Restore to original system (automatic mapping).
- The wizard does not require you to select all critical volumes displayed in the Source Disks/Volumes window to proceed, but for the recovery to succeed, you must select the volumes necessary for the operating system to boot. If you are unsure, select all critical volumes displayed in the window. You can select all critical volumes by highlighting the disk.

11 Add selected volumes to the Destination Disks window in the bottom half of the integrated BMR screen.

After highlighting the necessary volumes in the Source Disks/Volumes window, highlight the destination disk in the Destination Disks window. Then click **Add** to map the volume to the destination disk. To remove a volume, select the volume you wish to remove and click **Remove**.

Consider the following when selecting a destination disk for the restore:

- If you are restoring to a new disk, and this destination contains existing volumes, they are deleted during the restore and new volumes are created. If you are restoring to the original disks, only the restored volumes are overwritten. Other volumes on the original disk are not impacted by the restore.
- It is recommended that the destination disk be the same size as the original disk or larger to ensure that there is enough space for the critical volumes. However, the destination disk can be smaller than the original disk. Before initiating the recovery, you must make sure that the disk is large enough for the critical volumes; otherwise, the recovery will run until the disk is full, and then it will fail.

  Note: The disk/volume sizes displayed in the Source Disk/Volume window are the total capacity of the original disks/volumes and not the size of the backup that will be restored. After an asset has failed, there is no way to determine the size of its critical volumes. You can determine the size of an asset’s backup by viewing the backup details in the Backup History report on the Reports page. However, the size of the critical volumes will be smaller than the total size of a full backup if it also contains non-critical volumes. If you are unsure about the size of the backed up data on the critical volumes, it is recommended that you restore the failed asset to destination disks that are the same size as the original disks or larger.

- Volumes are assigned numbers during the restore that do not necessarily match the numbers from the original disk.

Click **Next** to proceed to the Execute the Restore screen.

To execute the integrated BMR

12 Click **Restore** in the Execute the Restore screen to start the restore.

The Integrated BMR Wizard assigns the restore a job number. You can monitor its progress in the Restore Progress window in the top half of the wizard screen or in the Status screen of the appliance where the backed up volumes reside.

The restore process can take several minutes.

13 After the critical volumes have been restored to the destination disk, you must inject an ESX or Hyper-V guest storage driver, depending upon your virtual environment. Click **Driver Injection**, and the Final Steps screen of the wizard displays.

Note: If you attempt to reboot without adding the driver, the VM will boot to a blue screen. You can return to the Integrated BMR wizard by booting from the disk containing the ISO image. The wizard will return to the first screen, and you can click ***Driver Injection*** and continue with Step 14 to inject the necessary driver.

14 Click the **Add Driver** button near the bottom of the screen.

15 Select the ESX or Hyper-V guest storage driver, and then click **Done** to add the driver to the list of drivers being injected.

16 To inject the driver, highlight the volume containing the operating system files in the window Asset's Offline Disk and Volume(s) Information. Then highlight the driver to add and click **Inject**.

17 When you receive a message stating that the driver injection was successful, you are ready to reboot the VM. Once the volumes have been restored, the Restore button in the wizard becomes a Reboot button. Click **Reboot** to complete the Integrated BMR Wizard.

After the VM reboots, you can restore data from the non-critical volumes that were not restored as part of the integrated BMR, as described in "Completing the integrated bare metal recovery" on page 31.

Post-restore driver injection

Note: This step is required only when restoring to dissimilar hardware.

If you are restoring to dissimilar hardware, or if a restored operating system fails to boot, you may need to inject drivers, so the operating system can communicate with the new hardware.

You must perform this procedure from within the Integrated Bare Metal Recovery Wizard. If you are continuing from step 14 of the procedure "Running the integrated Bare Metal Recovery Wizard" on page 22, you see the **Driver Injection** button on the screen that you used to restore the critical volumes. If you have booted from the integrated bare metal ISO after your restored operating system failed to boot, you are returned to the first screen of the wizard, and you can click **Driver Injection** in this screen.

Note: If you have returned to the wizard after your restored operating system failed to boot, do not use the Load Driver button under Load WinPE Drivers. This loads drivers into WinPE for the restore. Because your operating system has already been restored, you must inject drivers into this restored operating system instead.

To inject drivers into a restored operating system

1 Click **Driver Injection**.

2 Click the **Add Driver** button near the bottom of the screen. You can now browse for drivers to inject.

3 When you locate the necessary driver, select it and click **Done** to add it to the window labeled List of drivers being injected. Repeat this step as needed to add all the necessary drivers.

4 To inject drivers, highlight the volume containing the operating system files in the window Asset's Offline Disk and Volume(s) Information. Then highlight a driver to add and click **Inject**. Repeat this step as needed to inject all the necessary drivers.

5. When the wizard notifies you that drivers have been successfully injected, click **Reboot**.
6. When the restored asset reboots, you can restore data from the non-critical volumes that were not restored as part of the integrated BMR, as described in "Completing the integrated bare metal recovery" on page 31.

   Note: If the restored asset fails to reboot, you might need to add additional drivers.

Completing the integrated bare metal recovery

After you have restored the critical volumes, injected necessary drivers, and successfully rebooted your restored asset, use the steps described in this section to complete the recovery.

To complete the integrated bare metal recovery

1. Configure network settings for the restored asset. The network settings that you used for the restore in WinPE are not retained when you restore the failed asset’s operating system.

   Consider the following when configuring network settings for the restored asset:

   - If you assign it the same IP address as the failed asset, the backup system treats it as if it is the original failed asset.
   - If you are using DHCP to assign IP addresses and you registered the original asset to the backup system using only the asset’s name, the backup system detects the restored asset after you connect it to the network unless you rename it. The backup system then treats the restored asset as if it is the original asset.
   - If the original asset is still connected to the network, you must assign the restored asset a unique IP address and rename it before connecting to the network to avoid conflicts.
2. If necessary, you can now restore data that resides on non-critical volumes. For details, see Recovering Asset-level Backups. To restore data on non-critical volumes from a replication target, see Recovering Backup Copies. If all of your data resides on the critical volumes, then it has already been restored.
3. The backup system now protects the restored asset using the same settings it used to protect the failed asset. Existing backup and archive schedules for the failed asset are now applied to the restored asset. It is not necessary to create new schedules for the restored asset.

   Note: ***For Exchange servers.*** If you are unable to mount Exchange databases after performing the restore, the databases may be in a Dirty Shutdown state. See this Microsoft article for details: Exchange Database is in a Dirty Shutdown State.

   Note: ***For Hyper-V servers.*** After booting the recovered Hyper-V server, you must run the following command on the Hyper-V server:
   bcdedit /set hypervisorlaunchtype Auto. You should then reboot the server.

Performing a test integrated bare metal recovery

Before an asset fails, you can perform a test integrated bare metal recovery without impacting the original asset. As long as you assign the restored asset a unique IP address and rename it, the test recovery will not result in any network conflicts with the original asset. To perform the test recovery, use the procedures described in "Performing the integrated bare metal recovery" on page 19.

CAUTION! If you perform a test recovery and do not assign the restored asset a unique name and IP address, this will result in conflicts.

Chapter 3: Bare Metal for Linux

Use Unitrends bare metal protection for disaster recovery of your Linux assets. See the following topics for details:

- "Linux bare metal overview and requirements" on page 33
- "Implementing Linux bare metal protection" on page 34
- "Linux bare metal restore procedure" on page 35

Linux bare metal overview and requirements

To protect Linux assets, burn a bare metal .iso image to CD and run periodic master backups. For disaster recovery, boot from the CD, then restore the master backup followed by any differential and/or incremental backups. The most common situation necessitating a bare metal restore is when the entire file system on the Linux asset has crashed and cannot be recovered with the fsck command, but the system can be booted from the hard drive.

Linux hot bare metal recovery requirements and limitations

Keep the following criteria in mind when planning for Linux disaster recovery:

- For a list of supported Linux distributions, see the Unitrends Compatibility and Interoperability Matrix.
- A valid Master Backup of the asset must be performed before restoring from the boot CD.
- Linux bare metal protection does not support backups with inclusion lists.
- File systems cannot be removed from the configuration.
- Disks cannot be partitioned manually.
- Root disks cannot be changed.
- Linux hot bare metal protection does not support full disk encryption.
- The system must be restored to disks which are the same size or larger than the original disks.
- You are responsible for booting the system and the availability of the bare metal media.
- The computer can boot from the bare metal CD.
- Test the bare metal CD when created to make sure that it will work at the time of restore.
- The bare metal media for the server cannot be created after the system has crashed.

- The server must use the default service port of 1743. This is because the asset may not be able to modify its services file (/etc/services) when booted from the alternate boot media.
- Linux bare metal software will work correctly only if the asset has GRUB boot loader as the default. LILO boot loader is not supported.
- For VMware guests running Linux that were backed up at the GOS level, the VM must be configured to use the E1000 network adapter and its SCSI controller must use LSI parallel logic. Bare metal restore is not supported on Linux VMs using the VMXNET 3 adapter or whose SCSI controller uses VMware paravirtual. It is recommended to run backups at the host level rather than at the agent level.
- For assets with a default network adapter with a name other than eth0, you might need to edit the configuration file when creating the bare metal media. For details, see KB 1100.
- Dissimilar bare metal restores are not supported for Linux assets.

The premise of bare metal protection is to create a Linux bare metal boot disk, which contains programs, utilities, and system-specific information. This disk can be used to aid in recovery of a crashed system. The crashed system is booted using the bare metal disk to begin the restore process.

Bare metal restores the entire system from a selected master backup. All disks present in the system configuration during creation of the bare metal media are configured and used for restoring data.

Implementing Linux bare metal protection

To ensure your Linux systems are fully protected in the event of a disaster, implement bare metal protection as follows:

1. Install the Unitrends Linux agent and add the asset to the backup system. See Installing and updating the Linux agent for details.
2. Run periodic master backups. A valid master backup is required to perform bare metal restore of the asset. See Creating backup jobs for details.

   Note: Any backup group using an inclusion list is ineligible for bare metal recovery. Create bare medal media for the full disk. Inclusion lists can then be applied to asset aliases. For more information, see Managing physical assets under Managing protected assets.

3. Use the Unitrends console interface to create a bare metal *.iso* image. See "Creating Linux hot bare metal boot media" on page 35.

Creating Linux hot bare metal boot media

You can use your Linux master backups to create bare metal media, which can then be used to restore your server to similar hardware. Dissimilar bare metal restores are not supported for Linux assets. Ensure you have a successful master backup of the Linux server you wish to restore. This will be used to create your bare metal media. If you do not have a successful master backup of your Linux server, bare metal restore is not possible.

To create the bare metal boot media

> **Note:** For assets with a default network adapter with a name other than eth0, you might need to edit the configuration file when creating the bare metal media. For details, see KB 1100.

1. If you have a physical Unitrends appliance, insert a blank CD into the Unitrends system's optical drive. This is not necessary for a virtual Unitrends Backup appliance.
2. From the console interface of the Unitrends system, select option 4 - **Advanced Options**.

   > **Note:** You may remotely access the Unitrends system using an SSH asset and issue the command /usr/bp/bin/dpuconfig to access the console interface.

3. Select option 1 - **Bare Metal Media Creation**.
4. Select option 1 - **Linux Hot Bare Metal Media**.
5. Use the arrow keys to select the desired Linux asset.
6. The media is created. For physical Unitrends systems, it is burned to the media you inserted into the Unitrends system in Step 1. For virtual Unitrends systems, an .iso is created in the baremetals share, accessible from \\<IP of your Unitrends system>\baremetals.

Linux bare metal restore procedure

The Linux bare metal restore process uses a master backup of your server to recreate the operating system. All files associated with the master backup are restored. Files in any differential or incremental backups can be restored after the bare metal restore is complete.

It is important to know:

- You need a valid master backup, and the bare metal media should be tested as described in "Linux Bare Metal menu options" on page 37.
- The option Smart restore destroys all of the existing data on all disks. Please be sure that this is absolutely desired.
- The option to Make disk bootable in the Restore menu cannot damage anything on the disk.

To perform the restore

1. If performing the restore as a test, first see "Considerations for bare metal test recovery" on page 10.
2. Boot your new hardware from the disk you burned in "Creating Linux hot bare metal boot media" on page 35. If you need to change the IP of the restore target, navigate to **Utilities > Change IP addresses > Change Client IP address**. If you change the IP of the restore target, you need to change the relevant entry in the hosts file on the Unitrends system at this point as well. To do so, navigate to **Configure > Appliances(tab at top) > Network (tab at bottom) > Edit Hosts File** on the Unitrends interface.
3. You may optionally test connectivity to the Unitrends system by selecting **Test** from the menu.
4. Begin the restore process by selecting **Restore > Smart Restore**.

   Note: If the IP address of the Linux asset is changed before the bare metal restore process, the asset's IP address must also be updated in the Unitrends system's hosts file by navigating to **Configure > Appliances(tab at top) > Network (tab at bottom) > Edit Hosts File**

5. You are warned that the restore process will destroy all data currently on the disk you are restoring to. Type **Y** and press **Enter** to proceed.
6. Enter the name of your backup device and press **Enter**, or simply press **Enter** to accept the default. This is typically D2DBackups.
7. Enter ID number of backup to use. You may leave this blank and press **Enter** to use the most recent master.
8. Follow on-screen instructions to enter any exclusions. This data will not be included in your newly restored system. Type **none** and press **Enter** if you have no exclusions.
9. Review your choices and press **Enter** to proceed.
10. Your backup is transferred to your new hardware. Do not perform any actions on your new server until the restore is complete. You can monitor the status of this restore in the Unitrends interface by navigating to **Jobs > Active Jobs**.
11. Once the restore is complete, go back to your Linux server and press **Enter** to return to the Linux Hot Bare Metal menu. Select **Exit**, then select **Yes** to exit. If asked to make disk bootable, select **Yes**.
12. Your server reboots into its former state.
13. Perform file-level recovery to restore your machine to its latest backup. See Recovering Asset-level Backups for details.

Linux Bare Metal menu options

When booting the computer using the Linux bare metal media, the Hot Bare Metal interface displays. This permits the restore of an existing asset or allows information to be viewed regarding the configuration of the system's disks and file systems. Menu options are described in the remainder of this section.

Test

It is strongly recommended that the bare metal test be performed once the asset boots using the media. This can be done by selecting the Test option from the main menu. These tests establish a network connection to the backup system. After successfully testing bare metal media, store it in a safe location.

Restore

To restore your file system in the event of a disaster, select **Restore > Smart Restore**. This process automatically performs all necessary steps to set up the disk. **Restore > Prepare Disks** formats the disks. Your server is rebooted after the format is complete. **Restore > Make Disk Bootable** prepares the disk to be bootable and should be selected upon completion of the restore.

View Info

Using the View Information menu permits review of the mounted file systems, the file system table, mount points, disk partition information, the hosts, and the network routes.

Utilities

This option enables you to check the file systems on your disks, mount or unmount file systems, change the asset, system, and gateway IP address, and execute the UNIX shell.

Exit

Select **Exit** to exit the Linux Hot Bare Metal menu and reboot your server.

Initiate Linux asset restore from backup system

Use this procedure to manually initiate a bare metal restore of a Linux asset if a problem prevents the normal procedures from being used.

To perform a bare metal restore of a Linux asset

1. Boot the Linux server from the boot CD. Upon completion of the Linux bare metal boot process, the Linux Bare Metal interface displays.
2. Run the Test utility from the Linux Hot Bare Metal menu. This is important since the test utility not only checks the asset, it also starts the network.
3. Mount file systems by selecting **Utilities > Mount filesystems**.

4 To start the asset restore from the Unitrends interface, see Recovering Asset-level Backups.

Chapter 4: Bare Metal for x86 Platforms

The procedures in this chapter apply to all Intel-compatible platforms running on x86 architecture, other than Linux and Windows. For Linux and Windows clients, see "Bare Metal for Linux" on page 33 or "Windows Hot Bare Metal Protection" on page 13.

Cold bare metal backups are used to protect x86 platforms. To start, burn a bare metal ISO image to CD. Then run periodic cold bare metal backups by shutting down the asset, booting from the CD, and selecting the bare metal backup option from the boot menu. For disaster recovery, boot from the CD, then restore the bare metal backup followed by any file-level backups (master, differential, etc.).

See the following topics for details:

Intel platforms bare metal disaster recovery

Bare Metal Plus for Intel Platforms allows full crash recovery of any licensed backup system agent running on an Intel compatible PC platform. Bare metal backs up an asset’s main hard drive in a sequence of partition images. This version uses a Linux based bare metal boot media.

There are several fundamental things to understand about bare metal before getting started:

- Setup and configuration of some asset workstations must be done. This is because Bare Metal Plus is designed for crash recovery protection of client workstations, not the backup system.

- Bare Metal Plus only backs up the main hard drive on the first controller of the asset.
- The asset must have a CD-ROM drive.
- Bare Metal Plus supports bootable CD version.

The bare metal CD version creates an ISO CDROM image for a given asset. This image can then be used to burn a CD specific for each asset. It is suggested that you generate a CD for every asset and keep it in a sleeve next to the asset for emergency use in the event of a crash.

A hard disk attached to a PC is sectioned into areas called partitions. Each partition could be a separate operating system (such as Windows on partition-1 and UNIX on partition-2), or the disk could be split into file systems for a particular operating system. For example, Windows would make partition-1 the C: drive and partition-2 the D: drive. Bare Metal Plus will backup all partitions on the main disk without regard to their underlying operating system. We refer to this as an image backup.

The rationale behind image backups is:

- The system image backup is fast because it only backs up the real data on the drive, not empty blocks of unreferenced data.
- There are never issues with locked or open files when backing up the asset because the entire image is of a non-running, cleanly shutdown asset.
- The restore process is simple avoiding the complexities of installing and configuring specific operating systems.

Potential problems during a recovery are minimized due to its simplicity.

To create a bare metal boot CD

After the assets and D2D devices have been configured, create a bare metal boot CD for each asset which is bare metal aware. The bare metal boot media is created using the backup system's console interface. For physical systems, connect to the backup system console. For virtual systems, connect to the backup system VM within your hypervisor.

1. From the backup system's console interface menu, enter option ***4*** for Advanced Options, then ***1*** for Bare Metal Media Creation.
2. On the Bare Metal support screen, type ***2***, in the `Please enter choice` field for Cold Bare Metal Media.
3. Select the asset for which a bare metal backup needs to be done.
4. In the `Is the root disk on the client IDE? [Default is NO]` field, enter one of the following:
   - Leave this blank or type **N** to indicate the root disk on the asset is SCSI.
   - Type **Y** to indicate the root disk on the asset is IDE.

5. Enter the `Network Gateway` of the asset.
6. Enter **255.255.255.0** in the `Netmask` field.
7. In the `Is there a firewall between the asset and System?` field, enter **Y** to indicate there is a firewall or **N** to indicate there is not a firewall.
8. In the `Do you want your Cold Bare Metal backup to start automatically when booting from the CD that you have created?` field, enter **Y** to start the backup automatically or **N** if you do not want the backup to start automatically.

   The creation of the ISO begins automatically.
9. Once the ISO has been created, map the share on which the ISO was created and burn the ISO to a CD. The following prompt appears, telling you the location of the ISO and how to access it:

```
The CD (baremetal-<asset_name>.iso) has been created. Please map the CIFS
share \\<DPU_IP>\baremetals to access and burn the ISO.
```

Specifying bare metal settings for an asset

Follow the steps below using the bare metal Bootable CD dialog to specify settings for an asset on the backup system.

1. Select the asset from the **Bare Metal Client** combo box. Only Intel and Intel-compatible assets are listed. The backup system does not appear in this list even if it has an Intel CPU since Bare Metal Plus is only for assets.
2. Specify the Backup Device to use when performing manual bare metal backups. This can be a disk-to-disk device.
3. The **Is Root Disk SCSI** toggle determines whether the asset's primary disk is SCSI or IDE.
4. Specify the network options. Indicate whether there is a firewall between the backup system and the asset. Advanced network settings can also be specified which would contain the Netmask and the gateway information.
5. You may select **Add Another Asset** and repeat the above process to configure additional assets to run on the same bare metal CD.
6. Click **Create Bare Metal CDROM** image.
7. Click **Save** to save the profile.

The images of the assets are stored in the following directory, where $*BPDIR* is the installation directory of the backup software (which is */usr/bp* by default):

```
$BPDIR/cdrom_images
```

The software checks to ensure there is enough free space in the /usr/bp partition for the creation of the ISO images. The creation of the ISO images requires approximately 25MB. The image can be transferred to a CD and used for the bare metal of the asset. After the creation of the image, a message is displayed to inform the user about the last backup for that asset.

If a previous bare metal backup does not exist, use the crash recovery media to perform a bare metal backup of the system. Once the CD is created, use it to boot the asset. If multiple clients are configured on the CD, a list of machine names are provided to select the appropriate client. If the CD is created only for one asset, an unattended bare metal backup can be performed. For an unattended backup the software waits for 30 seconds before a bare metal backup is queued at the server. If the countdown is interrupted, then the Main Menu system is displayed with various options.

Bare Metal Plus supports:

- Bare metal bootable CD and the combo CD with an updated set of drivers. This greatly facilitates in detecting new hardware. The drivers are current with the latest Fedora release.
- You can manually change the root drive from the **Utilities > Set Root Drive** option. This feature helps you change the root drive from the standard hda or sda to the actual drive that is to be backed up. This feature plays a crucial role in the case where there is a zip drive attached to a lower SCSI ID than the root disk. In this case, now the root drive can be explicitly set to backup the appropriate drive.
- A Troubleshooting Menu has been added to facilitate problem solving when a problem situation occurs. This menu shows useful information, such as SCSI devices that are attached to the system, network configuration, modules loaded by the bootable operating system, and information about the hard drive such as geometry, size, and model type.
- Software ida and cciss devices.
- Bootable CD and CD/floppy combination for multiple assets to be configured on the same crash recovery media.
- Multiple network cards. It automatically detects and configures the appropriate card.

Testing bare metal backups

Please test your bare metal backup strategy for each asset by performing a bare metal restore of the asset to a test system. Testing and documenting bare metal restore in your environment will insure quick responses and successful bare metal recovery when required.

Recovering from a crash with the bare metal boot CD

Every registered asset should have a bare metal crash recovery media created as soon as it is set up. Typically, bare metal backups should be done every month or whenever any major changes (hardware or software) are made to the asset. To do a bare metal backup, boot the asset using the bare metal CD.

To restore a bare metal backup, you must have created the Bare Metal Plus crash recovery media and a bare metal backup.

To restore a crashed system using the metal boot CD

1. Boot the asset from the media.
2. Restore the bare metal backup to the asset.
3. Reboot the asset using its normal operating system.
4. Restore the last master backup to the client.
5. Restore the last incremental backup that was performed after the last master backup, to the asset. This may not be necessary if no incrementals have been done since the last master.

Using the bare metal crash recovery boot CD

When the asset system boots up from the CD it shows a list of assets on that CD if more than one is present. Select the asset that you want to restore by using the arrow keys, and then press **Enter**.

A dialog displays asking you to wait until the settings have been applied. This may take a while. At this point the network and hard drives are detected and configured for use. After these settings have been applied, a message box displays.

Steps on the above message are necessary only if a hot bare metal is to be performed. Press any key after reading the message to get to the main menu. Use the arrow keys to move from one menu option to another. Press **Enter** on the option you wish to select.

After the asset boots up, click **Utilities > Bare Metal Quick Test** to conduct the Bare Metal Quick Test. This set of tools make sure the hard drive is detected correctly. It tries to check the network connection to the server and tries to ping it by name and IP address. If all tests are successful, the system is ready for performing bare metal backups and restores.

The failure of any of these tests is indicated by the status *Failed*.

If Phase 1 (Test for Hard Drive) or Phase 2 (Test for Network) fails, go to **Utilities > Advanced > Confirm** hardware detection menu option. This displays the root drives as well as the network interfaces of the system and allows the user to change them if incorrect.

If Phase 3 (Ping server by name) or Phase 4 (Ping server by IP) fails, go to **Utilities > Advanced > Change Settings** to change the IP address of the server.

If Phase 5 (Test connect BP server) fails, make sure that the backup system's service is listening on the appropriate port (1743).

See "Bare metal boot CD menu options" on page 44 for a description of the options displayed in the menu.

Bare metal boot CD menu options

The following options are available in the bare metal boot CD menu:

- "Bare metal boot CD tasks option" on page 44
- "Bare metal boot CD backup option" on page 44
- "Bare metal boot CD restore option" on page 45
- "Bare metal boot CD utilities option" on page 45

Bare metal boot CD tasks option

The Tasks Option provides Real Time Statistics and a Real Time Task Monitor.

The Real Time Statistics dialog shows the real time statistics of the currently running bare metal backup.

The Real Time Task Monitor is similar in functionality to the Task Monitor on the backup system. It displays the task number, the asset name, and type of action taking place, the device on which the backup is taking place, the tape number, the current status and a comment on whether the task is completed.

Bare metal boot CD backup option

Select **Backup > Backup** for the backup screen to display.

The Bare Metal Backup dialog displays the name of the asset and the server. These fields cannot be altered.

The Server backup **Device** field allows you to enter the backup device being used.

Verify the backup? field is used to determine if a backup will be verified. Bare metal backups should be done at least once a month.

To exclude a partition, select **Exclude Partitions** and press **Enter**. A list of partitions displays. Use the up-down arrow keys to select a partition and press the space bar to check the box.

A backup comment can be added if desired. Press **F6** to start a backup.

Bare metal boot CD restore option

Restore All – This option queues a restore job on the server and restores all the partitions.

Restore Master Boot Record (MBR) – This option allows you to restore only the master boot record from the backup.

Restore MBR and Extended MBR – This allows the restore of the master boot record and the extended MBR from the backup selected.

Restore Selected Partitions – This option allows you to select specific partition(s) to restore. The **Select Partitions** field allows you to select partition(s) to restore. The default is none. Press **Enter**, and use the space bar to check or uncheck the partition.

Note: A bare metal backup cannot be restored to a smaller disk.

All the restore options mentioned above have the same restore fields.

The Asset name and the Server name are not editable.

Server Backup Device allows you to change the device name, if required.

Backup Number allows you to select the backup number to restore. By default this is **0**, which indicates the last successful bare metal backup. If you know the number of the backup you want to restore, you can change this number.

Press **F6** to run the restore.

Before a selective partition restore is performed, the partitions have to be created. If a restore is being done to a blank hard drive, then restore the MBR/EMBR first and then restore the selected partition. You could use fdisk to create the partitions as well. If the partition is larger than the one in the backup, the restore does not restore the partition. You will have to use some third party application to restore the partition.

Bare metal boot CD utilities option

Select Client: This option is used only if the boot CD has multiple assets. If you select **Yes** to the question asked about configuring the asset, a list of assets displays. Choose the asset you wish to configure. A hostname and the network for this asset is also configured.

Bare Metal Quick Test: See the section on Quick Test to view details.

Escape to UNIX Shell: This takes you to a UNIX shell prompt where you can perform command line functions and then exit back to the Bare Metal interface.

Disk Utilities: This option provides a set of utilities to change the root drive if the one detected is not the correct drive, a utility to partition the disk, cleanup the Master Boot Record, and some statistic information about the disk. Disk Utilities has these options:

- fdisk to root disk: This option allows you to view information about the partitions on the system. You can also use this option to partition the drive if the restore is being done to a new disk.
- Zap the MBR: This will clean the Master Boot Record which holds the information about partitions and the boot record. This should be used with caution since this will render the system unbootable. Make sure you have a good bare metal backup before performing this operation.
- View Hard Drive: Allows you to view the information about all the hard drives on the system.
- Set root drive: This option allows you to set the appropriate root drive if the one detected is incorrect.

Troubleshooting: This menu allows you to view the system configuration in detail. It shows information about network configuration, the devices detected during boot up, and also allows you to set the speed of the network card if desired.

View PCI Bus: This option displays all devices that are attached to the PCI bus.

View Loaded Modules: This option displays all the loaded modules on the system.

View SCSI Devices Attached: This displays the SCSI devices attached to the system.

View Network Settings: This option displays the network card configuration. If there are several network cards, the one connected to the server would be configured.

Change Network Settings: This option allows you to change the settings for any network card. The **Restart Autonegotiation** option tries to configure the network to autonegotiation mode. By default it is set to no.

The Force Speed option allows you to set a speed. Select the option and press **Enter** to view a drop-down list. The force speed options are 10Mbps, 100Mbps, 1000 Mbps.

Force Mode sets the mode to be Half or Full Duplex.

Logs: This menu option allows you to view or delete the bare metal logs.

View Bare Metal Logs: This menu allows you to view the startup logs, the bare metal logs, or a log of a particular file.

Delete Logs: This option allows all the log files to be deleted.

Advanced: This option has the following parts:

- Change settings – As seen the asset and server IP settings can be changed. While doing the Bare Metal Quick Test, if there is a failure in phase 3 or 4 (ping server by IP and name), you can check the settings and if incorrect, set the correct IP address. The netmask and the gateway can also be altered if required.

- Confirm hardware detection– This option helps you identify the hard drives and network on the system. If the root drive has been identified correctly, select **Yes** to display all network interfaces. Again you are asked to identify whether the network interface is correct. If both the root drive and the network interface have been correctly identified, it performs the Bare Metal Quick Test.

  Note: This function must be done for hot bare metal to function properly.

- Backup Entire Disk – This option is used to back up the entire disk instead of backing up the partitions on the disk. This option should be used in cases where the system is configured for Software Raids (Dynamic Disks or GPT partitions in Windows).
- Exit – This allows you to exit out of the Bare Metal Menu.

Manual bare metal backup

Follow the procedures to create the crash recovery media as explained in the above sections in its entirety. Once the crash recovery media has been created, insert it into the asset and reboot the PC. The asset will boot from the CD, assuming the BIOS is configured to do so. A banner displays on the screen to warn you of an impending automatic backup (the default). Press the Enter key to interrupt the Automatic Backup countdown if any manual adjustments need to be made to how the backup is performed. The main Metal Plus menu then displays where you can choose the Backup option to gain more control over the process. Otherwise, allow the count down to expire and the machine will complete the backup and prompt you to reboot to the normal operating system.

When to perform a cold bare metal backup

System retention rules retain one bare metal backup per asset per week. It is recommended, at a minimum, to perform a bare metal backup of the assets every 30 days or anytime a patch is installed or software is upgraded on an asset. A bare metal backup for an asset should also be performed anytime a new network or primary hard disk (SCSI, IDE) hardware is added or any significant configuration changes are made to the server. In order for a crashed machine to boot and work properly after a bare metal restore, make sure all the new settings are present on the server. Test the new settings by booting from the newly made metal crash recovery media and make sure that the network and disk have been properly recognized. To do this, go to **Utilities > Advanced > Change Settings**.

Recovering from a crash using cold bare metal

To restore a bare metal backup, you must first have a Bare Metal Plus crash recovery media *and* the last master and differential (if applicable) backups for the asset. Follow the procedures in the above mentioned sections to create the media for the asset you want to restore.

To restore a crashed system using Metal Plus

1. An asset Metal Plus crash recovery media should be available with you.
2. Boot the asset with the media. To get more details about the usage of the bare metal boot CD, see "Intel platforms bare metal disaster recovery" on page 39.
3. Restore the bare metal backup to the asset.
4. Interrupt the automatic backup so that the Bare Metal Plus menu displays.
5. Remove the bare metal media and reboot the asset using its normal operating system.
6. Restore the last master backup to the asset.
7. Restore the last differential backup that was performed after the last master backup, to the asset. This may not be necessary if no differentials have been done since the last master.
8. Once the restore is done, remove the media.

Basic bare metal restore procedures

1. Boot the asset using the bare metal crash recovery media. Press the **Enter** key when you see the Automatic Backup countdown to proceed to the main menu.
2. Select **Restore** from the main menu. This takes you to the restore menu. From the restore menu you can restore:
    - Everything
    - Just the master Boot Record (MBR)
    - Selected partitions
    - The system and disk info file
3. Select one of the restore options and you will be asked a few simple questions and then the restore will be queued to the backup system.
4. After having restored the system, reboot to the newly restored operating system and restore the last master and incremental backups.

Bare metal restore to a new disk

Special considerations must be taken when restoring to a new disk. You must be aware of how the new drive differs from the original. For instance, is the new disk larger or the same size as the old one? Is the new disk SCSI and the original was IDE? When should you restore the Master Boot Record (MBR)? The MBR is the first part of the drive that contains the partition layout and data used to boot the server. These considerations are discussed in the next section.

Note: A bare metal backup cannot be restored to a smaller disk.

Bare metal restore to a disk of same size and controller

This is the simplest restore. Boot from the bare metal media and follow the "Recovering from a crash using cold bare metal" on page 47.

Bare metal restore to a larger disk

You must partition the drive before performing a restore whenever restoring to a new disk on the same controller (i.e. new and original disks are either both SCSI or both IDE) that is a different size than the original. From the restore menu, choose option **Restore** and **View System/Disk Info** to restore and view the sizes of the original disk before it was last seen by a bare metal backup. Write these numbers down.

Using the original disk sizes, make new partitions using option **FDISK the Main Drive** from the main menu. This creates a new MBR. When creating the new partitions, it is OK to make them bigger than the original, but if made smaller, the restore will have problems fitting all of the data onto a given partition.

This type of restore requires restoring using the option **Restore Selective Partitions**. Otherwise, if **restore all** is selected, the MBR will be restored, which will undo the work you did using FDISK to partition the drive.

Bare metal restore to a different disk controller

A different controller means that the system was backed up on an IDE disk and you are now restoring to a SCSI disk or vice-versa. If this is the case, you must specify the new disk controller in the Create Bare Metal for Assets dialog for the asset, and then create the Bare Metal Plus diskette. Use the new diskette to boot the asset, then follow the steps in "Bare metal restore to a larger disk" on page 49.

Configuration settings for CD only version of bare metal

These settings are present in the master.ini file in $BPDIR/bpinit.

UseAlternateImage – By default this option is set to **False**. On some servers or specific hardware, the default image might experience problems during the boot. To work around this problem we have another set of drivers that can be used for booting. After setting this flag to **True**, recreate the media for the asset. This option must be set to **True** if the asset machine is a Compaq Server.

ForceCDBurn – If the server is configured for burning ISO images using the cdrecord package, then this option can be set to **True**. Enabling this option allows you to burn the image from the graphical Administrator Interface.

CdromDeviceID – This field specifies the SCSI ID of the CDROM drive. The ID can be obtained by running the command **cdrecord -scanbus** as a shell prompt. Our software determines the SCSI ID internally and defaults to this field if it cannot identify the drive.

Bare metal optimization

Bare Metal Plus backups can take quite some time on large disks if not optimized before the backup. Optimization can dramatically decrease the time of a bare metal backup. Optimizing the disk takes about one minute per 500 megabytes of data on a slow Intel computer. In contrast, to backup 500 megabytes of unused data to the backup system could take as much as three minutes plus the space used on the disk.

The optimization process notes the unused space on a disk so that compression will be maximal. This process must be performed on the running asset before the metal backup has begun.

To perform optimization of a Windows asset, you can access this as a choice under the Options section of the main agent menu.

Optimization of UNIX assets is performed using the following command:

```
/usr/bp/bin/bputil -X
```

Consider optimization periodically for each asset metal backup. The period chosen depends on the amount of disk activity on the asset. A good time to consider optimization is when a large number of files have been deleted from the asset's main disk drive.

Novell agent bare metal optimizer utility

The Bare Metal Optimizer utility (bmopt) is useful when using the add-on bare metal product installed on the server. This option allows for the optimization of a system so that the bare metal backups perform at peak speed and size. This utility displays block-level statistics for all the volumes on a NetWare Server. In a user friendly manner, it provides a facility to check and purge all deleted but not purged blocks on a volume, reducing the size of bare metal backups to optimal size, if ran on all volumes prior to bare metal backups.

The available disk blocks on a NetWare server, at any given time, fall into two categories: *free* and *purgeable* blocks. The space consisting of free blocks do not contain any files. Purgeable blocks hold deleted files. A deleted file is not actually removed from the disk instantly, but merely marked as *purgeable*. The deleted file still occupies space on the volume and consumes directly entries. NetWare translates purgeable-blocks into free-blocks at a low priority. It runs a low priority task to scan all volumes, to purge the deleted blocks.

When a bare metal backup runs at a block level it cannot differentiate between real blocks associated with existing files and purgeable blocks, resulting in large sized backups since the bare metal is backing up deleted files. The bmopt utility can be used to resolve the issue.

BMOPT displays a list of all non-admin volumes, and corresponding block-level statistics:

- No. of Available Blocks
- No. of Purgeable Blocks
- No. of Total Blocks on a server

It can optimize the available space, and reflect the same in a corresponding volume's block level statistics. Depending on the number of purgeable block on a volume, you can decide to run optimization on a volume.

Usage

```
LOAD SYS:\BP\BMOPT.NLM
```

To select a volume, use the Up and Down Arrow Keys and select **Enter** to begin. Any progressing optimization process can be canceled by selecting **ESC**. To exit the tool, select **ESC**.

Chapter 5: Bare Metal for non-x86 Platforms

This chapter provides bare metal procedures for platforms that are not built on the x86 architecture. To protect non-x86 compatible platforms, burn a bare metal ISO image to CD and run periodic master backups. For disaster recovery, you boot from the CD, then restore the master backup followed by any differential and/or incremental backups.

See the following topics for details:

Bare metal for AIX

To protect AIX assets, burn a bare metal ISO image to CD and run periodic master backups. For disaster recovery, you boot from the CD, then restore the master backup followed by any differential backup.

AIX asset hot bare metal restore

Bare metal restores are supported for AIX 5.3 and higher. (For a complete list of Unitrends supported AIX versions, see the Unitrends Compatibility and Interoperability Matrix. Bare metal restores allow you to recover an AIX asset due to system failure. Bare metal requires that you create the bare metal media on the asset. This media can then be used to aid in recovery of a crashed system.

Bare metal restores the entire system from the most recent master backup. All disks which are included in the system configuration at the time the bare metal media was created are configured and data restored.

Key points for protecting your system:

- Bare metal media should be generated whenever there is a significant change to the system.
- Bare metal media should be tested to make sure that it will work at the time of a system restore.
- You must have a good master backup of the asset before restoring from the boot media. Do not exclude system files that are required for a system to boot.
- The bare metal media for a system cannot be created after the system has crashed.

Generating bare metal media for an AIX asset

Bare metal media is created by running the mkbmcd utility on the asset. This utility is found in *$BPDIR/bin/mkbmcd*, where *$BPDIR is /usr/bp* by default. The creation utility is invoked from the shell with:

```
$BPDIR/bin/mkbmcd
```

The mkbmcd requires that you enter the following information:

- Temporary workspace directory – This directory should have 500000 blocks available.
- Storage directory for iso image – This directory should have 500000 blocks available.

If enough space is not available on the asset machine, create an NFS share on the backup system and mount it on the AIX asset. For details see Procedures for adding external storage.

Starting the bare metal restore for an AIX asset

Boot your computer using the AIX bare metal media. This will allow you to restore your existing asset or view information about the configuration of your disks and file systems.

Note: By default, the AIX system does not boot from the CD drive. The system configuration should be changed to boot from the CD drive. This can be done during the boot process.

Bare metal for AIX menu options

Access the bare metal for AIX menu by booting from the AIX bare metal media. Menu options are described in the remainder of this section.

Bare metal for AIX test option

It is recommended to run the Bare Metal Test once the asset boots using the media. This can be done by selecting **Test > Test** from the Main menu. This operation tests the mount/unmount of the hard drive, network connection to the backup system, and starts the TCP/IP listener (daemon) to check if it is ready.

Bare metal for AIX restore option

If recovering after a system crash, select **Restore > Smart Restore**. The process will perform all necessary steps automatically to set up your disk. You will be asked to specify the system's backup device and backup number. To restore the last master backup, do not enter a backup number response, i.e., leave it blank.

At the end of a restore, you are prompted with the following:

You may need to make your root disk bootable.

Do you want to do it now? (y/n) [y]

Answer **y** or press **Enter** to accept the default. If you have performed a step by step restore, the option **Make disk bootable** should be selected before exiting.

Another way to restore a system is to perform a step by step restore. Each of the following steps is required to successfully complete the restore. From the restore menu, select **Format partition > Create Filesystem > Restore files > Make disk bootable**.

View AIX asset information option

Using this menu allows you to review important system settings which were saved during the creation of the bare metal CD. **View Info** displays the mounted file systems, the filesystem table, mount points, disk partition information, the hosts, and the network routes.

AIX asset utilities option

This menu allows you to mount / unmount, check, and change the asset and server IP address, select an alternate hard disk, and run UNIX shell.

Initiate AIX asset restore from backup system

The following instructions can be used to manually initiate a restore if a problem prevents the normal procedures from being used:

1. Run **Test** on the asset.
2. Format disk and create file systems if necessary.
3. Mount file systems.
4. From the Administrator Interface, choose the backup for the asset to restore. While viewing the details of the backup, choose **Restore** located in the lower right area of the screen.
5. Click **Show Advanced Execution Options** to open the form.
6. Make sure that the Target Directory is set to:

   ```
   /tmp/root.mnt
   ```

   This is the directory where the bare metal application has mounted the root filesystem on the asset.
7. Press **Restore** to initiate the restore. You may use the Job Status screen in the to view the progress of the restore.

Reasons for AIX bare metal restore

The bare metal software is a powerful and flexible tool. In many cases, you do not really need to use all of its features. However, you should understand how to apply bare metal in the quickest and most effective way. Let's consider a few common cases when a system may need to be restored.

- An important file (directory) on the system has been corrupted or removed.

If your system is on the network, you do not need your bare metal media. Simply perform a Selective Restore from the backup system and select only the file(s) you need.

- The system is dead. The root drive has been formatted or replaced. Something unknown happened to the computer and now it does not work, it cannot be booted.

Boot your system using the AIX bare metal boot CD. From the main menu select **Restore > Smart Restore**. This reconfigures all of the disks and restore all the files.

Important things to know about bare metal restores:

- The option **Smart Restore** destroys all of the existing data on all disks. Please be sure that you really need this step. Make sure also that you have a valid master backup and your bare metal media was tested successfully.
- The option **Create filesystems** on the Restore menu removes all of the files from that filesystem. You will be prompted if you really wish to do this.
- The option **Format Partitions (Automated)** removes all existing data.
- The choice **Make disk bootable** in the Restore menu cannot damage anything on your disk.

Bare metal for Mac OS X

The topics below describe support for hot bare metal recovery on Mac OS X. They cover installation of the protection software for Mac OS X, steps necessary to create a Mac OS X hot bare metal boot DVD, and instructions for using such media to restore a master backup.

- "Hot bare metal diaster recovery using Mac OS X" on page 56
- "Creating hot bare metal Mac OS X boot media" on page 57
- "Mac OS X hot bare metal restore" on page 58

Hot bare metal diaster recovery using Mac OS X

Protection of the Mac asset begins with the creation of an ISO file that captures information about the system running in its natural state. This ISO image file is then burned to a hot bare metal DVD that can be used to recover a system in the case of disaster or unrecoverable crash.

From this disk you boot into the recovery environment and restore the system and files to the state that existed before the crash.

Technical limitations and requirements

Unitrends supports hot bare metal restore for computers with the following Mac operating systems: Mac OS X 10.5 through Mac OS X 10.11. For a complete list of Unitrends supported Mac OS X versions, see the Unitrends Compatibility and Interoperability Matrix.

Note these hot bare metal limitations:

- Dissimilar bare metal restore is not supported on any Mac OS X at this time.
- The following file systems are supported: HFS and HFS+.

Creating hot bare metal Mac OS X boot media

To recover a protected system, a hot bare metal USB drive or DVD must be created on the computer being protected. A few things to keep in mind:

- The hot bare metal media should be tested after creation to make sure it will work when a system needs to be restored. The media can be tested by selecting the Test option on the Mac OS X Hot Bare Metal v.60 interface. See "Mac OS X hot bare metal restore" on page 58 for accessing this menu.
- A full backup of the client is required prior to doing a hot bare metal restore. Full backups can be performed from the appliance UI or from the backup menu.
- The hot bare metal media cannot be created after a system crashes.
- The computer's (asset's) hostname should be registered on the backup system.

Use one of the following procedures to create the boot media:

- "To create the Mac OS X boot media for 10.10 and 10.11"
- "To create the Mac OS X boot media for 10.9 and earlier versions"

To create the Mac OS X boot media for 10.10 and 10.11

1. Place an empty 8GB or larger USB drive in the computer's media drive.
2. Connect to the Mac asset by using a terminal emulator (such as PuTTY) and log in as user root or administrator.
3. Enter the working directory where the ISO file will be built.
4. Run the Bare Metal utility by entering `mkbmcd` from the location where the Mac agent is installed. Example commands are given here:
    - For Mac 10.10, the default agent location is /usr/bp. For an agent installed in that location, enter this command:

```
/usr/bp/bin/mkbmcd
```

- For Mac 10.11, the default agent location is /usr/loca/bp. For an agent installed in that location, enter this command:

  ```
  /usr/local/bp/bin/mkbmcd
  ```

5 When the ISO image is complete, the following message displays:

```
The newly created iso image is present at the location.
```

6 Determine the disk number of the USB drive by entering this command:

```
diskutil list
```

7 Enter the following command to burn the ISO image to the USB drive, where the *X* is the disk number of the USB drive:

```
dd if=<image> of=/dev/rdiskX bs=1m
```

To create the Mac OS X boot media for 10.9 and earlier versions

1 Place a blank DVD in the computer's media drive.

2 Connect to the Mac asset by using a terminal emulator (such as PuTTY) and log in as user root or administrator.

3 Enter the working directory where the ISO file will be built.

4 Run the Bare Metal utility by entering `mkbmcd` from the location where the Mac agent is installed. For Mac 10.9 and earlier, the default agent location is /usr/bp. For an agent installed in that location, enter this command:

```
/usr/bp/bin/mkbmcd
```

5 When the ISO image is complete, the following message displays:

```
The newly created iso image is present at the location.
```

6 Enter the following command to burn the ISO image to a disk:

```
hdiutil burn /<path>/bm_<hostname>.iso.cdr
```

Mac OS X hot bare metal restore

To recover a system using the hot bare metal DVD, perform these steps:

1 Load the hot bare metal DVD, boot the computer and hold down the **Option** key until the boot menu loads.

2. Choose the boot media using the mouse or arrow keys.
3. Press the following keys simultaneously, until the boot message displays:

```
Command+S+Return
```

4. To start the Mac OS X Hot Bare Metal interface, at the command prompt enter:

```
./init
```

   It will take a few minutes for the system to start up and launch the interface.

5. From the Restore Menu, select **Smart Restore**.
6. When the warning displays that all data will be destroyed, select **y** to proceed.
7. After the file systems have been created, the Restore Now screen loads. Enter the name of the backup device or press **Enter** to accept the default device.
8. At the next Restore Now screen, provide a backup number or press **Enter** to use the last master backup.
9. Enter exclusions if necessary, or enter **None** if there are no exclusions.
10. At the summary screen, verify the Server, Device, and Backup Number are correct.
11. Press **y** to continue.

From here the status of the restore process can be monitored from the Administrator Interface.

Bare Metal for Solaris SPARC

To protect Solaris SPARC assets, burn a bare metal ISO image to CD and run periodic master backups. For disaster recovery, you boot from the CD, then restore the master backup followed by any differential backup. Details are given in the following topics:

- "Solaris SPARC bare metal restore" on page 59
- "Generate and boot from the bare metal media" on page 60
- "Bare metal recovery from a Jump Start boot server" on page 63

Solaris SPARC bare metal restore

The Solaris SPARC asset bare metal restore enables rapid recovery of the Solaris SPARC asset to the most recent state of the system. It is the optimal method of recovering a complete system in the case of catastrophic failure. Unitrends provides support for Solaris 9, Solaris 10, and Solaris 11 (with update 8 or update 9). In addition bare metal boot from a USB drive is supported for Solaris 10.

The premise is to first create an iso image that captures pertinent information about all programs, utilities, and the state of the system at the time the image is created. This iso image is then burned to a CD and can be used to aid in recovery of a crashed system.

General technical notes:

- Bare metal media cannot be created after the system has crashed.
- It is imperative to test bare metal so you know it works when needed.
- The supported operating systems all have means of alternate booting.
- It is important that you become familiar with alternate boot procedures so the machine can be booted in the case of a disk failure.
- You are responsible for the means to boot the system and the availability of the bare metal media.
- Bare metal media should be generated whenever there is a significant change to the system.
- A good master backup of the client must exist before restoring from the boot media.
- Do not exclude system files that are required for a system to boot.
- Bare metal restore is not supported to dissimilar target hardware.

Generate and boot from the bare metal media

Before using the bare metal restore process, the media must first be created and tested on the targeted Solaris SPARC asset.

Bare metal restores the entire system from the most recent master backup. All disks which are included in the system configuration at the time the bare metal media was created are reconfigured and the data restored.

Prerequisite: Solaris 9, Solaris 10, or Solaris 11 (with Update 8 or Update 9).

Creating and booting from the bare metal CD

To generate the bare metal iso image file

1. As root, run the **mkbmcd** utility on the asset, which is found in *<INSTALLDIR>/bin/mkbmcd*, where *<INSTALLDIR>* is */usr/bp* by default.
2. Initiate the creation utility by entering the following at the command prompt:

   ```
   /usr/bp/bin/mkbmcd
   ```
3. When prompted by the mkbmcd utility, enter the temporary workspace directory, which requires:

   - 275MB of space for Sun 4U architecture
   - 550 MB of space for Sun 4V architecture

4. When prompted, enter the storage directory for the iso image, which requires:
   - 275MB of space for Sun 4U architecture
   - 550 MB of space for Sun 4V architecture
5. Locate the ISO image in the designated storage directory and burn that image to a CD.

Note: If enough space is not available on the asset machine, an NFS partition on the Unitrends System can be created and mounted on the Solaris SPARC asset to store the iso image. See Procedures for adding external storage for details.

To boot from the bare metal CD

By default, the Solaris SPARC system does not boot from the CD drive without one of the following commands. This allows the existing asset to be restored or viewed, including information about the configuration of disks and file systems.

To boot the computer with the bare metal media, use either of the following options:

```
reboot -- cdrom // if at the command prompt
```

or

```
boot cdrom // if in OpenBoot
```

Creating and booting from a bare metal USB drive

Requirements:

- The hardware must include a USB 2.0 port.
- Open Boot firmware must be 4.27 or greater.
- Before plugging in the USB drive, make certain Volume Management is disabled. The command for this is:

  ```
  svcadm disable volfs
  ```

To generate bare metal media on a USB drive

1. Run the mkbmcd utility on the asset which is found in *<INSTALLDIR>/bin/mkbmcd*, where *<INSTALLDIR>* is */usr/bp* by default.
2. Initiate the creation utility by entering the following at the command prompt:

   ```
   /usr/bp/bin/mkbmcd
   ```

3. When prompted, indicate **y** when asked if you want to use USB Bare Metal Recovery.

   Note: This erases all content on the drive.

4. When prompted by the mkbmcd utility, enter the temporary workspace directory, which requires 550MB of space.
5. When prompted, enter the asset and backup system information.
6. When prompted, select the desired USB drive by entering the corresponding number.

   Note: Device Type must be removable disk.

7. When prompted, confirm the listed information and begin the formatting process by entering **y**.

   Once the process is complete and the drive has been formatted, the following message appears:

   ```
   Please follow the instructions below to boot from the USB drive:
   ```

8. Remove the USB drive from your machine.
9. Enter ‘*# init 0*’ to get to the ok prompt.
10. Plug in the USB drive and enter ‘*probe-scsi-all*’.
11. ‘Locate the SCSI address for the Removable Disk Entry.

    Append

    ```
    /disk@0,0
    ```

    to the end of the SCSI address.

    Example:

    ```
    /pci@0/ pci@0/ pci@1/ pci@0/ pci@1/ pci@0/usb@0,2/storage@3/disk@0,0
    ```

12. Boot the USB drive using the SCSI address with

    ```
    /disk@0,0
    ```

    appended to it.

    Example:

    ```
    boot /pci@0/ pci@0/ pci@1/ pci@0/ pci@1/ pci@0/usb@0,2/storage@3/disk@0,0
    ```

    The system boots from the USB drive and starts the Bare Metal Application. You must have a master backup of this system before you can perform a bare metal restore.

Bare metal recovery from a Jump Start boot server

Solaris bare metal recovery can be performed from a Jump Start server. In this case, a bare metal recovery can be performed without the use of a cdrom or USB media. If the Solaris server is configured to communicate with a Jump Start boot server, a bare metal recovery can be performed.

Requirements

Network boot for bare metal recovery is only supported on SPARC Solaris version 2.10. Please note that the Jump Start server and the protected Solaris server are required to be on the same version.

The protected Solaris server (and OpenFirmware version) must support network boot.

Prerequisites

The Solaris system and the Jump Start boot server should be on the same subnet.

To boot the protected server using the Jump Start boot server, it is required that the Jump Start server is configured and the protected Solaris server is added as a asset to the Jump Start boot server.

The protected Solaris agent can be added to the Jump Start boot server by running the following command on the Jump Start server boot server:

```
add_install_asset -e <Ether address> -s sunv240:/<location of boot server>
<hardware class> <hostname>
```

In the command above:

- Ether address – This is the ethernet (MAC) address of the protected Solaris system. This information can be obtained by running *ifconfig –a* on the protected Solaris server.
- Location of boot server – This is the location of the top level directory on the Jump Start server where the boot server is installed and configured.
- Hardware Class – This is the hardware class of the protected Solaris server and can be obtained by running *uname –m* on the protected Solaris server.
- Hostname – This is the hostname of the protected Solaris server and can be obtained by running the hostname command.

Example:

```
add_install_asset -e 0:3:ba:f4:7e:15 -s sunv240:/boot_server sun4u SunT5220
```

Setup

On the protected Solaris server

1. Run the mkbmcd utility on the asset which is found in *<INSTALLDIR>/bin/mkbmcd*, where *<INSTALLDIR>* is */usr/bp* by default. Initiate the creation utility by entering the following at the command prompt:

   ```
   /usr/bp/bin/mkbmcd
   ```

2. When prompted, indicate **n** when asked if you want to use USB Bare Metal Recovery.

3. When prompted, enter the information (name and IP) of the protected asset and the information (name and IP address) of the backup system.

   The setup process piggybacks on the process to create an ISO, as described in the section above. When prompted, provide the path to the storage area to save the resulting ISO.

A sparc.miniroot file needs to be installed / copied to the Jump Start server in order to perform a network boot operation. Perform the following steps to copy the space.miniroot file to Jump Start server.

1. Create a loopback device with the iso created as mentioned above:

   ```
   lofiadm -a <full-path-to-BM.iso>
   ```

2. Mount the bare metal iso:

   ```
   mount -F hsfs <looback block device> <mount point>
   ```

3. After mounting the iso the sparc.miniroot can be copied to the boot server by doing the following:

   ```
   scp <mount point> /boot/sparc.miniroot <user>@<bootServer>:<path-to-boot-
   server-directory>/boot/sparc.miniroot.<hostname>
   ```

   Example:

   ```
   scp /tmp/sparc.miniroot.SunT5220 root@BootServer:/boot_
   server/boot/sparc.miniroot.SunT5220
   ```

Booting into the bare metal interface

When performing a bare metal recovery, please perform the following steps to boot into the Bare Metal recovery interface via the network.

1. On the Jump Start boot server, copy the sparc.miniroot.<hostname> file as sparc.miniroot (save the original sparc.miniroot file before performing this step).

2. On the protected Solaris server, at the Open Firmware prompt type:

```
boot net
```

The Solaris server boots into the Bare Metal recovery interface and is ready for performing the restore as described in "Performing a bare metal recovery" on page 65.

Performing a bare metal recovery

To perform the restore, perform the following steps:

1. Select **Test > Test** from the Main menu.

   This operation tests the network connection to the backup system and verifies that the Solaris asset and the backup system can communicate to perform the bare metal recovery.

2. Select **Restore Options > Smart Restore**.

   The restore process recreates the disk, partition, and file systems structure for all the disks identified when the bare metal media was created.

3. When prompted, specify the backup device and backup number.

   Note: To restore the last master backup, simply press ***Enter***. A restore job will be queued to the backup system and the status of the restore can be monitored from the Job Status screen.

4. At the end of a restore, you are prompted with the following:

   ```
   You may need to make your root disk bootable.
   ```

   ```
   Do you want to do it now? (y/n) [y]
   ```

5. Answer **y** or press **Enter** to accept the default.

Bare metal for Xen virtual machines

A bare metal backup of a Xen virtual machine is captured in a manner supported by the guest operating system on the virtual machine. For example, on a Windows Server 2008 virtual machine, a hot bare metal backup can be scheduled and performed as described in the "Windows Hot Bare Metal Protection" on page 13.

Restoring a bare metal image to a virtual machine requires specific steps to be taken to access the bare metal menu on the bare metal boot CD. These same steps would be taken to access the bare metal menu to perform a cold bare metal of a virtual machine.

The protection software creates a fully virtualized mock virtual machine to be used to communicate with the system to backup and restore a bare metal image from or to the appropriate location.

> **Note:** This requires that the server CPU supports a fully virtualized environment and that VT/AMD-V is enabled in BIOS.

The virtual machine that is going to be backed up or recovered must be shutdown during the bare metal process.

To access the bare metal menu from a bare metal boot CD, perform the following steps:

1. Know the exact name of the virtual machine to be backed up or recovered. The existing virtual machine names can be found using the virtual machine management GUI or executing this command from the command line:

   ```
   xm list
   ```

2. Insert a bare metal boot CD in the host system's CD drive. The bare metal boot CD should have been created for the specific guest virtual machine(s) following the instructions provided in the Bare Metal section.

3. From a command line on the host system, run this command:

   ```
   /usr/bp/bin/start_bare_metal <VMName><Device>
   ```

   Where <VMName> is the name of the guest virtual machine to be backed up or recovered and <Device> is the name of the device in which the bare metal boot CD is inserted. For example:

   ```
   /usr/bp/bin/start_bare_metal sles10 /dev/cdrom
   ```

   > **Note:** Run ***mount*** at a command prompt as root or root equivalent user to verify the device name of the cdrom.

   When the command runs, a mock virtual machine is created and will be used to backup or restore images of the actual virtual machine to be protected or recovered. The following text displays on the screen:

   ```
   #########################################################
   CREATING PLACE HOLDER FULLY VIRTUALIZED VM FOR BARE METAL
   #########################################################
   Checking Processor(s) ...:
   [ Supports Full Virtualization. ]
   Checking Kernel ...:
   [ Running XEN Kernel:2.6.16.46-0.12-XEN ]
   Checking status of XENd ...
   [ XENd running (pid 4177 4180) ]
   Configuration file for the VM ...
   /etc/XEN/vm/sles10
   ```

```
Creating Profile ...
Using config file "/usr/bp/mock_conf".
VM: unitrends_Bare Metal created.
```

The new virtual machine is now running and the bare metal menu displays. A bare metal image backup or recovery can be performed following the steps detailed in the applicable bare metal section for the VMs operating system. To find the desired procedure, see "Bare metal procedures by asset operating system" on page 9.