

# Problem

HOWTO: Use NetBackup to perform a restore for a total and complete recovery of Windows client(s) that include C: (and other system) drive(s), Shadow Copy Component, and/or System\_State from a reliable full MS-Windows backup without IDR or BMR in the event of a Disaster (or need to fall back to a known working state).

# Solution

Use NetBackup to perform a restore for a total and complete recovery of Windows client(s) that include C: (and other system) drive(s), Shadow Copy Component, and/or System\_State from a reliable full MS-Windows backup without IDR or BMR in event of Disaster.

## **How to use this guide:**

This guide is provided as a general/generic template that would be applicable for most restores, and may require trial-and-error and multiple attempts. Most of the time using the following steps the way it is, will result in good bootable system.

The guide is intended for restore back to the original machine. If the machine is damaged and replaced with another machine (regardless of being 99.999% identical make/model) this is no longer considered the original machine. You may attempt to treat it like an original restore (using w2koption), but there is a risk that restore will result in a non-bootable system (if this is the case, retry without w2koption). For non-original system restore do not use w2koption. If target is not the original, the larger the difference from the original machine, the lower the success rate of a bootable system.

This guide is NOT intended for system cloning. It is intended for Disaster Recovery of a client back to original hardware, or a near identical new hardware should the original no longer be available.

## **Pre-Requisites**

- This is for a client system restore only.
- This procedure will restore your computer's system files and data files to a pre-

disaster state except those protected by one of the NetBackup database agents, such as the Exchange agent or SQL agent. If any of your data is protected by NetBackup agents, refer to the section on restoring the data protected by the agent before beginning disaster recovery.

- This procedure does NOT utilize NetBackup Bare Metal Restore (BMR) or NetBackup Intelligent Disaster Recovery (IDR) but instead makes use of standard Windows-NT backups of all local drives including System\_State (Windows 2000 and earlier AND NetBackup 4.5 and earlier) or Shadow Copy Components (Windows 2003 and later AND NetBackup 5.1 and later).
- Any Windows 2003 (or later) client backed up previously by NetBackup client 4.5X would not support Shadow Copy Components restore. You must select only System\_State. This is true trying to restore from an OLDER version 4.5X backup even if the client has been upgraded to 5.X or later.
- The success of a full restore will depend on a "reliable" full system backup. So if System State or Shadow Copy Components backups complete with a Status 1, then it is not reliable for a Disaster Recovery Scenario.
- This procedure requires third party Windows 2000 or 2003 Setup media from Microsoft in order to perform reinstallation of the operating system. The same version/suite must be used. For example, if the original version is Windows Enterprise Server 2003 with Service Pack 1, that same version must be installed for disaster recovery. All related hardware drivers that are required to reinstall Windows and configure networking must be available and ready. Network functionality after windows is booted up is a requirement. **NOTE: For a higher success rate, install the same drivers (and applications which install drivers) the system had when the backup was made. Failure to do so can result in a post-restore reboot loop.**

- For Windows 2003 clients (any variants e.g. SP1, SP2, R2, x86, x64), make sure it already has Microsoft VSS patch KB940349 installed prior to restore. If not, download the patch from <http://support.microsoft.com/kb/940349>, install and then reboot the server before proceeding.

**WARNING:** You cannot recover using a different Windows OS than was previously installed. For example, Windows 2003 Small Business could not be used to recover a Windows 2003 Enterprise server.

**NOTE:** You may have to [re]install drivers even after a successful restore and reboot.

**NOTE:** When using an imaging software to rebuild the box, please verify it is supported by Microsoft.

### **Other options to consider:**

- NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. For a complete description of BMR backup and recovery procedures, see the Bare Metal Restore System Administrator's Guide.
- If you installed and configured NetBackup Intelligent Disaster Recovery (IDR) on the client system, refer to the NetBackup Administrator's Guide, Volume II, for recovery procedures instead of the instructions below.

### **Solution:**

#### **1. Setup and Install Windows.**

Install the original version of Windows. This basic Windows installation is necessary to provide NetBackup with a target to which it can restore the system. The computer name, Windows directory, and the file system type (such as NTFS) must be the same as it was on the previous Windows installation. This installation will be overwritten by the recovered version, which will restore your original system configuration, application settings, and security settings. After setup, install the necessary service packs to bring Windows to the same level as was previously installed.

**NOTE ABOUT HARDDRIVE PARTITIONS:** If you are recovering from a disk failure,

use Windows Setup to partition and format the new disk during installation. Use **the same** partition layout **or larger** as was on the previous drive. If smaller partition sizes are configured, this can cause a restore failure and or BSOD on boot post-restore. Format the partitions with the same file system type as before the failure.

#### **NOTE ABOUT DOMAINS DURING SETUP:**

- If the system was in a specific domain or workgroup, do not join the domain or workgroup at this time.
- If you are recovering a domain controller, do not perform the domain controller installation process at this time.

## **2. Configure Network.**

Reinstall Network Interface Card (NIC) drivers (same version) if Windows does not have built-in support for the NIC. The same IP and hostname must be used.

**NOTE:** Consult your Windows administrator, network administrator, NIC hardware/installation manual and/or NIC vendor support channel for additional information regarding driver support and configuration under Windows.

## **3. Install NetBackup Client.**

Install the same version of the NetBackup Client for Windows as it was during the backup, including any necessary patches. Do not install a newer (higher) version than the master server.

If the client version is not known, the version file (<install\_path>\VERITAS\NetBackup\version.txt) can be restored from the backup image of the client to an alternate location on the master or a media server and examined.

**RECOMMENDATION:** Perform a custom installation where NetBackup is not installed to the same drive as Windows. If you have to reformat and perform a Windows installation again, you will not lose access to NetBackup client logs.

## **4. Enable NetBackup client logs:**

A. Navigate via Windows Explorer to your <Program Files>\Veritas\ folder. This

represents the custom drive letter and folder name you used during the custom installation of the NetBackup client. Example: D:\Program Files\Veritas\.

B. Navigate into the *NetBackup* folder, and then into the *logs* subfolder. If this subfolder does not exist, create it.

C. In the *logs* folder, create these three subfolders: *bpineta*, *bpca*, and *ta*.

D. Open the Backup, Archive and Restore (BAR) GUI console from the client: Start > All Programs > Veritas NetBackup > Backup, Archive and Restore

E. Select File > NetBackup Client Properties > Troubleshooting (tab).

F. Under Debug Levels, set General to a value of 2 and Verbose to a value of 5.

G. Stop/Restart the NetBackup client service via the Windows Services console. (Start > Run > type *services.msc*) Find NetBackup Client Service, highlight, and Stop. After it has stopped, restart it with Start.

## 5. Start the restore process.

**NOTE:** For this procedure to work, the restore must **not** be initiated from the Client. Rather, initiate the restore from the Master Server or Remote Admin Console.

A. Launch the **Symantec NetBackup BAR** (Backup, Archive & Restore) GUI application.

B. First, select the images that contain the Full and Incremental (if applicable) backups of the system drive first(s). Enable the overwrite option. **Do not elect to restore the System State/Shadow Copy Components at the same time.**

**NOTE:** "System drive(s)" in modern day may no longer be just "C:" drive; as it is becoming more and more common to custom build and tune Windows to place system components into different drive for scalability and performance benefits. When considering restoring a client that was customize in this way, it is important to restore not only the C: drive, but all other drives and folders where system components are needed by Windows to operate. For example, this may include part or all of "Program Files" if some system dependent application is installed on elsewhere, for example security services or anti-virus. During boot time, Windows may have been configured to load critical libraries that could be located in custom install paths outside of C:

**WARNING: DO NOT REBOOT** after the system drive(s) restore is completed.

C. When the restore is complete, check the client's tar log (found in <Program Files>\Veritas\NetBackup\logs\tar ) for confirmation of a successful restore. If the restore had errors, this log will provide more detail and any issues found should be resolved before continuing.

D. System\_State/Shadow Copy Components.

**CAUTION:** This is the most critical part of the restore that could result in a bootable system or non-bootable system.

Select the images that contain the Full and Incrementals (if applicable) backups and start a restore of the System State/Shadow Copy Components with the overwrite option enabled.

**NOTE:** By default, the System State/Shadow Copy Components assumes the restore is to different hardware (and NOT the original machine) and does not restore the registry hive:

HKLM:\System\CurrentControlSet\Control\BackupAndRestore\KeysNotToRestore.

This will result in the loss of certain hardware driver and configuration information noted by Microsoft here: <http://technet.microsoft.com/en-us/library/cc737538.aspx> (this means you may have to [re]install drivers if restore/reboot is successful).

If the restore being attempted is to the ORIGINAL hardware and you wish to restore this information, use the W2koption.exe utility supplied with the NetBackup Windows Client. **THIS SHOULD NOT BE USED IF RESTORE IS NOT TO ORIGINAL HARDWARE.** Running W2koption.exe:

**NOTE:** below is an updated procedure used and referenced from: <http://www.symantec.com/docs/TECH22365>

1. If this is not the original system, skip this step, otherwise, before the restore of System\_State or Shadow Copy Components component starts, run the w2koption with the following command syntax: (No need to run below command for Win 2008 Clients )

```
<install_path>\VERITAS\NetBackup\bin\w2koption -restore -same_hardware 1
```

2. Then, restore the System\_State or Shadow Copy Components. **DO NOT REBOOT THE SERVER YET.**

3. Repeat the w2koption command as done earlier: ( No need to run below command for Win 2008 Clients )

<install\_path>\VERITAS\NetBackup\bin\w2koption -restore -same\_hardware 1

**NOTE:** For Windows 2003, if shadow copy was successfully restored and still NOT able to boot, on next try, instead of restoring the entire or Shadow Copy Components, simply expand and just select System\_State portion; and skip w2koption.

**NOTE2:** If you want to restore Shadow Copy Components or System\_State again to the original hardware and recover device driver information, you use repeat the w2koptions steps before and after again.

E. Upon completion of the restore, check the tar log again for any problems. Once again, **DO NOT REBOOT**.

## 6. Double-check.

Double-check to see if there is any System data on other drives that needs to be restored. At this time, if there is any, restore it.

## 7. [Optional] Restore other data.

Perform restores of other drive letters (non-system Drives) before rebooting. (Alternatively, you could perform this step after the reboot.)

## 8. Stop the service named "NetBackup Client Service" or "NetBackup Legacy Client Service".

**NOTE:** After the Restore job completes, the NetBackup process named **bpineta.exe** has pending registry-merge responsibilities post-restore. It will perform the queued registry-merge tasks upon graceful shutdown of the process. Killing the process (bpineta.exe) using Task Manager or other tools will prevent the registry merge from happening. This will cause a post-restore boot failure.

To verify the post-restore registry manipulation is completed there are 3 options:



## **RECOMMENDED**

**NOTE:** The log specific to steps 8.1 and 8.2 is ...\\NetBackup\\logs\\bpinetd

**8.1. NBU 7.0 and older:** Manually Stop the *NetBackup Client Service*. **This will cause bpinetd.exe to perform the merge operation and terminate gracefully.**

**When bpinetd is no longer running,** it should be okay to reboot the system. The following command can be run to stop the NetBackup Client Service:

```
net stop "NetBackup Client Service"
```

**8.2. NBU 7.1 and newer:** Manually Stop the *NetBackup Legacy Client Service*. **This will cause bpinetd.exe to perform the merge operation and terminate gracefully.**

**When bpinetd is no longer running,** it should be okay to reboot the system. The following command can be run to stop the NetBackup Legacy Client Service:

```
net stop "NetBackup Legacy Client Service"
```

## **NOT RECOMMENDED**

**8.3. Simply shutdown/reboot the OS like normal.**

**When the OS shuts down running Services, bpinetd.exe should shutdown gracefully and perform the registry merge operation.**

**NOTE:** Step 8.3 above works in the majority of situations. However, in rare circumstances when the OS brings down services (upon reboot), the bpinetd.exe process can not complete the post restore registry actions before the process is terminated during the reboot sequence. When this happens, a reboot-loop will be observed. Frequently, the reboot will not be associated with a BSOD, but will simply POST in the middle of the boot process. If this behavior is observed, manually stopping the services (as described in steps 8.1 and 8.2) prior to reboot will allow the bpinetd.exe the needed time to perform the registry merge operation before reboot.

## **9. Transfer logs from restore before rebooting!**

Transfer the client's NetBackup logs to an area where you can access them if the post-restore reboot fails.

## **10. Post Reboot Action.**

After the reboot, if a blue screen occurs while the client is starting Windows, attempt to boot using Safe Mode (or Safe Mode with Networking). If a Safe Mode Boot succeeds, take a look at the Windows event logs, and export them. Transfer them to another

partition (or network location if Networking is enabled and working under Safe Mode).

If there is no alternate method to access and transfer data, reinstall the operating system again and set up Networking so evidence can be sent to the Technical Support of various vendors, including Symantec for NetBackup support.

**NOTE:** If you took a chance and restored to a non-original machine with w2koption, retry this procedure again (reinstall/rebuilding Windows also) and skip over w2koption. If it still fails to boot and this is Windows 2003, retry again without w2koption AND only restore System\_State from Shadow Copy Components.

**NOTE:** The first boot after doing a full OS restore of Windows 2008 or Windows 2008 R2 may take 5-10 minutes or longer. It may show a blank screen during this time. The machine is not hung. Do not reboot forcefully during this time, as it may corrupt the OS causing it not to boot up. The slow boot is due to a bulk file-rename for files which were restored with temporary file names because their production counterparts were active and locked at the time of the restore. This also happens with Windows 2003, but the file-set is much smaller and the boot-lag is therefore much shorter in duration.

Terms of use for this information are found in Legal Notices.