VSS Plugin

Bacula Systems Documentation

Contents

Contents

1 Backing up Windows Machines

In general, there are three distinct ways Windows machines can be backed up with **Bacula Enterprise**:

- Backup Windows as an image. This requires shutting down the Windows system, rebooting a Linux system (CDROM or USB) and then backing up the raw Windows partition or partitions using a Linux File daemon running on the Linux system. Since this method requires shutting down the Windows system, booting a Linux system, then backing up the raw partitions, it is rather labor intensive. Each backup is the full size of the Windows partition or partitions (disks). In addition, you cannot do file level restores; only the full image can be restored. The advantage is that a restore is quite fast. We will not explore this option any more in this white paper.
- Normal Bacula Windows backup without the VSS plugin. This is a standard backup where you back up everything on every disk with the exception of temporary files. This backup uses VSS (default Bacula option), but not the VSS plugin. Bacula has worked in this manner for many years, the code is stable and many users have restored user files and done many successful Bare Metal Recoveries. In fact, Bacula Systems has a separate WinBMR tool that automates this technique for Bare Metal Recovery.

  This normal backup must be done **without** the Bacula VSS plugin, although Bacula will use Windows VSS APIs (but not the VSS plugin) to create a snapshot of the filesystem that is then backed up. Normally such a backup includes all the operating system files.

The disadvantage of this normal backup is that you cannot easily restore individual components of the System State as you can with the VSS plugin. However, you can do two kinds of restores:

1. A restore of standard user files or any system files that are not in use by the OS (most are in use and cannot be restored while the system is running).
2. A Bare Metal Recovery.

   During a Bare Metal Recovery, you can restore the whole system including all the System State files. The disadvantage compared to the VSS plugin restore is that you must restore the whole system rather than individual components. Note: it is also possible to restore any subset of the files rather than all files, so if you have expert knowledge of System State files, you could potentially restore only the System State or any other system component. In practice very few people would be inclined to do this.

- Backup the System State and / or several other system elements such as MSSQL, Exchange, etc. These are described in detail in this white paper. The difference between this kind of a backup and the previous item described above is that this approach uses the Bacula Enterprise VSS plugin.

  A backup that uses the Bacula Enterprise VSS plugin should be a separate Job from a normal user file backup (see above). The advantage of this kind of backup is that if your system state is damaged, you can restore the particular element that is broken or the full system state while the system is running then reboot to complete the process.

  The disadvantage of this kind of backup is that it cannot be used for a Bare Metal Recovery. This is because any backup containing data written by the VSS plugin requires VSS for its restores, and Microsoft does include neither the VSS subsystem in WinPE, which is used for bare metal recovery, nor can the recovery environment handle any other VSS-aware application like MSSQL Server or Exchange, since those can not be available and configured during a Bare Metal restore.

- The VSS plugin is compatible with Copy/Migration jobs. Please read the CopyMigrationJobsReplication for more information.

Summary: Bacula provides several methods of backing up and restoring Windows filesystems. As mentioned above, the most common is simply to backup everything *without* the VSS plugin. Normal restores can then be done on any file that is not locked by the system (mostly user files) while the system is running, or you can shutdown the system and do a Bare Metal Recovery where normally, all files are restored.

The rest of this white paper will discuss the Bacula Enterprise VSS plugin for **Bacula Enterprise** version 6 and newer and how to use it.

2 Bacula Windows VSS Plugin

We provide a single plugin named **vss-fd.dll** that permits to back up a number of different components on Windows machines. Components that are supported currently include:

- **System State writers**
  - Registry
  - Event Logs and Performance Counters
  - COM+ REGDB (COM Registration Database)
  - System (Systems files – most of what is under c:/windows and more)
  - WMI (Windows Management and Instrumentation)
  - NTDS (Active Directory)
  - Task Scheduler
  - Dhcp Jet (DHCP status and leases)

  - FSRM (File Server Resource Manager) data

- **Exchange**. Please note, there is an older Bacula community Exchange plugin that works entirely differently (it uses an old Exchange API rather than VSS). This old community Exchange plugin (**exchange-fd.dll**) is not discussed here.
- **MSSQL databases** Backing up and restoring MSSQL databases works very well for Full and Differential backups. It is not possible to do Incremental backups because backing up an MSSQL database uses block differencing, which requires Differential backups.

  Note that experience shows that large and busy MSSQL Server instances may often not be able to be backed up using VSS. In those situations, the **Bacula Systems** SQL Server VDI Plugin will provide a more reliable solution.

Each of the above specified Microsoft components can be backed up by specifying a different plugin command line within the Bacula FileSet. All specifications must start with **vss:** and be followed with a keyword which indicates the component, such as **/@SYSTEMSTATE/** (see below).

To activate each component you use the following:

- **System State writers**

```
Plugin = "vss:/@SYSTEMSTATE/"
```

  Note, exactly which subcomponents (writers) will be backed up depends on which ones you have enabled. For example, on a standard default system only COM+ REGDB, System State, and WMI are enabled. The plugin automatically finds all subcomponents (writers) that are enabled and will list them in the Job report.

  The Windows ASR Writer is automatically disabled by the plugin because Bacula Systems uses its own Bare Metal Recovery techniques.

- **Exchange**

```
Plugin = "vss:/@EXCHANGE/"
```

  The Exchange writer supports Full, Differential, and Incremental backups. For more details on the Exchange component of the VSS plugin, please see our white paper for Exchange with Bacula Enterprise version 6.0.

- **MSSQL databases**

```
Plugin = "vss:/@MSSQL/"
```

  Note, MSSQL backup works only for Full and Differential backups.

The plugin directives must be specified exactly as shown above. A Job may have one or more of the **vss** plugin components specified.

You must ensure that the **vss-fd.dll** plugin is in the plugins directory on the FD doing the backup (done by default with the installer), and that the **Plugin Directory** directive line is present and enabled in the FD's configuration file bacula-fd.conf.

If the plugin is loaded can be verified by checking the `status client` output with a debug level set, which shows the available plugins. An example session should look like this, where the line starting with "Plugin" shows which plugins are available, including the **vss-fd** one:

```
*setdebug level=1 client=wsb-exch10-fd
Connecting to Client wsb-exch10-fd at wsb-exch10:9102
2000 OK setdebug=1 trace=1 hangup=0
*status client=wsb-exch10-fd
Connecting to Client wsb-exch10-fd at wsb-exch10:9102
```

(continues on next page)

(continued from previous page)

```
wsb-exch10-fd Version: 6.0.0.5 (06 Mar 2012)  VSS Linux
Cross-compile Win64
Daemon started 19-Mar-12 11:44. Jobs: run=0 running=0.
Microsoft Windows Server 2008 R2 Standard Edition Service Pack 1
(build 7601), 64-bit
VSS enabled, Priv 0x22f
APIs=OPT,ATP,LPV,CFA,CFW,
 WUL,WMKD,GFAA,GFAW,GFAEA,GFAEW,SFAA,SFAW,BR,BW,SPSP,
 WC2MB,MB2WC,FFFA,FFFW,FNFA,FNFW,SCDA,SCDW,
 GCDA,GCDW,GVPNW,GVNFVMPW
 Heap: heap=0 smbytes=23,678 max_bytes=23,678 bufs=75 max_bufs=75
 Sizeof: boffset_t=8 size_t=8 debug=1 trace=1 mode=0,2010 bwlimit=0kB/s
Plugin: alldrives-fd.dll delta-fd.dll vss-fd.dll

Running Jobs:
Director connected at: 19-Mar-12 11:45
No Jobs running.
====

Terminated Jobs:
====
*setdebug level=0 client=wsb-exch10-fd
Connecting to Client wsb-exch10-fd at wsb-exch10:9102
2000 OK setdebug=0 trace=1 hangup=0
```

Newer versions of **Bacula Enterprise** report the plugins loaded even without the debug level being set. With the debug level set, they will report the plugins internal version number, like this:

```
wsb-master-fd Version: 6.2.7 (08 July 2013)  VSS Linux Cross-compile Win64
Daemon started 12-Sep-13 13:09. Jobs: run=5 running=0.
Microsoft Windows Server 2008 R2 Standard Edition Service Pack 1
(build 7601), 64-bit
VSS enabled, Priv 0x73f
APIs=OPT,ATP,LPV,CFA,CFW,
 WUL,WMKD,GFAA,GFAW,GFAEA,GFAEW,SFAA,SFAW,BR,BW,SPSP,
 WC2MB,MB2WC,FFFA,FFFW,FNFA,FNFW,SCDA,SCDW,
 GCDA,GCDW,GVPNW,GVNFVMPW,LZO
 Heap: heap=0 smbytes=154,611 max_bytes=40,440,895 bufs=112 max_bufs=59,514
 Sizes: boffset_t=8 size_t=8 debug=1 trace=1 mode=0,2010 bwlimit=0kB/s
 Plugin: alldrives-fd.dll(1.1) delta-fd.dll(1) vss-fd.dll(1)
winbmr-fd.dll(3.0.12)
```

The details of doing backups and restores with the **vss** Exchange component are discussed in a separate White Paper entitled **ExchangePlugin-6.0** (which covers any **Bacula Enterprise** version 6 and newer).

Please take note of the comments above concerning the difference between this VSS plugin (**vss-fd.dll**) with the Exchange component selected and the older community Exchange plugin (**exchange-fd.dll**).

2.1 BMR and VSS

The VSS plugin will not work correctly during a Bare Metal Recovery because Microsoft does not include the VSS subsystem in WinPE. As a consequence, any backup you do with the **vss** plugin cannot be used for a bare metal recovery. To have a good backup for bare metal recovery restore, you must run the Bacula FD **without** the **Plugin =** directive in your FileSet (i. e. the plugin must be turned off).

3 Backup

If everything is set up correctly as above then the backup will include the system state. The system state files backed up will appear in a **bconsole** or **bat** restore like:

```
/@SYSTEMSTATE/
/@SYSTEMSTATE/Registry Writer/
/@SYSTEMSTATE/COM+ REGDB Writer/
etc
```

Only a backup of all the system state subcomponents is supported. That is it is not possible to just back up only one subcomponent such as the Registry or NTDS alone. In almost all cases a complete backup is a good idea anyway as most of the components are interconnected in some way.

Both Differential and Incremental backups are supported.

Windows does not update the time and date of modification on all system files, so if you want correct Differential and Incremental backups, you **must** use the Bacula **Accurate** option. If you do not use this option, the plugin will print a warning message.

The Full backup size varies according to your installation. Backup sizes of a few GB under Windows Server 2003 and up to 20 GB under Windows 2008 are typical, mostly because of the "System" writer. The actual size depends on how many Windows services (writers) are enabled.

The system state component automatically respects all the excludes present in the Windows **FilesNotToBackup** registry key, which includes things such as %TEMP%, `pagefile.sys`, , etc. Each plugin component may automatically specify additional files to exclude, e. g. the VSS Registry Writer will tell Bacula to not back up the registry hives under `C: WINDOWS system32 config` because they are backed up as part of the system state backup.

4 Restore

In most cases a restore of all the backed up system state subcomponents is recommended. Individual writers can be selected for restore provided the whole writer is selected. To restore just the Registry, you would need to do **mark Registry*** to mark the Registry writer and everything under it.

Restoring anything less than a whole writer will cause the restore Job to fail with an error message.

When doing a restore, you must do a restore of the current system (i.e. option 5 on the restore menu) or a restore to a point in time. You should not attempt to select individual JobIds for restore, because to do a proper restore, one must choose all jobs that were previously run from the Full Job up to the point in time. If any JobIds or files are skipped as might happen if you choose the JobIds yourself, the restore may fail.

If you want to restore multiple subcomponents, we recommend that you do them all together or do a restore of the whole System State component.

If you are trying to restore a writer (component) to a different machine, please be aware that Bacula Systems does not support this, because as far as we can tell, it is not supported by Microsoft. This seems to be because most writers are

integrated with or rely on Active Directory, and so if you do not have exactly the same Active Directory environment on the alternate machine, the restore is not likely to work correctly.

Bacula Systems do not yet support restoring any component that is configured in a Microsoft cluster. You are free to try it, but according to the Microsoft documentation, there are a good number of restrictions and requirement for doing restores in clustered environments. If you succeed in backing up and restoring in a clustered environment, please let us know as we will be very interested in your results.

4.1 Reboot Required After Restore

After the restore of certain System State components, you must reboot before the changes can be properly applied. Bacula will print a message in the Job report indicating when this is necessary. The reboot is required because some VSS components will restore files that are currently in use. However, since files that are in use cannot be deleted, modified, or replaced, a reboot will be required to complete the restore by moving those restored files in place. Once you have restored such System State component, you must reboot your machine.

Until the reboot, the system will be in an unstable state, so please do not forget this step. In particular, starting another restore of VSS data after a restore requiring a reboot without first rebooting will cause any subsequent VSS plugin restore Job to fail.

4.2 Restore to Alternate Locations

Restore to alternate locations is not implemented in the **vss** plugin, nor is file name mangling using regular expressions.

4.3 Restoring Active Directory

To restore Active Directory, the system will need to be booted into Directory Services Restore Mode, an option at Windows boot time. Consequently, restoring Active Directory is a bit complicated. You might want to read Microsoft's comments about doing restores (note: their comments about Backup tools do not, in general, apply to Bacula).

technet.microsoft.com/en-us/library/cc961934.aspx

Bacula Systems can provide more detailed help regarding restoration of NTDS data; please contact our support team if you require that advice.

You need to be aware of Directory Services Restore Mode, the difference between authoritative and non-autoritative AD restores.

One important thing to consider is that, if you've got more than one AD server in your domain, you probably never have to go through the recovery procedure in practice, as it's easier to just set up a fresh server rather than doing an AD recovery, make the new server an AD server, and let it pull its data through replication from the existing servers. In other words, using backed up AD data should be considered a last-resort, disaster-recovery only approach.

4.4 Example

Suppose you have the following backup FileSet:

```
@SYSTEMSTATE/
  System Writer/
    instance_{GUID}
    System Files/
  Registry Writer/
    instance_{GUID}
```

(continues on next page)

(continued from previous page)

```
    Registry/
  COM+ REGDB Writer/
    instance_{GUID}
    COM+ REGDB/
  NTDS/
    instance_{GUID}
    ntds/
```

If only the Registry needs to be restored, then you could use the following commands in **bconsole**:

```
cd @SYSTEMSTATE
mark "Registry Writer"
```

5 Windows Plugin Items to Note

- Reboot required after a plugin restore In general after any VSS plugin is used to restore certain components, you may need to reboot the system. This is required because in-use files cannot be replaced during restore time, so they are noted in the registry and replaced when the system reboots.
- Longer boot time after a restore After a System State restore, a reboot will generally take longer than normal because the pre-boot process must delete the old files and move the newly restored files into their final place prior to actually starting the OS. For a large system, this can take quite a long time (we have seen up to 20 minutes).
- One file from each drive needed by the plugin must be backed up At least one file from each drive that will be needed by the plugin must have a regular file that is marked for backup. This is to ensure that the main Bacula code does a snapshot of all the required drives.

  Available as of version 8.0.1

  An alternative approach is to use the `alldrives` plugin, or, with **Bacula Enterprise** version 8.0.1 or newer, the **File=/** semantic in the file set.

  Available as of version 12.6.0

  Since version 12.6.0, the `alldrives` plugin or a file on every drive that will needed by the plugin are not necessary anymore.

- Bacula does not automatically backup mounted drives. Any drive that is mounted in the normal file structure using a mount point will not be automatically backed up by Bacula. If you want it backed up, you must explicitly mention it in a **File=** directive in your FileSet, or use the **File=/** semantic mentioned above.
- The VSS plugin does not work with WinBMR When doing a backup that is to be used as a Bare Metal Recovery, do **not** use the VSS plugin. The reason is that during a Bare Metal Recovery, VSS is not available nor are the writers from the various components that are needed to do the restore. You might do a full backup to be used with a Bare Metal Recovery once a month or once a week, and all other days, do a backup using the VSS plugin, but under a different Job name. Then to restore your system, use the last Full non-VSS backup during the bare metal restoration of your system, and after rebooting do a restore with the VSS plugin to get everything fully up to date.

- Restoring components to a different machine that is not identical (or, in some cases, nearly identical) to the machine on which the component was backed up is not supported.
- ---

  Available as of version 12.6.0

  Backup of clustered volumes (csvfs) is supported.

- The `estimate` command does not work with the VSS plugin. When estimating a job that uses plugins, an error message regarding the plugin will be displayed.
- Some programs such as Windows Defender are protected from external operations. It is not possible for the SYSTEM service account to restore Windows Defender files. Using WinBMR and the Live CD can restore files.
- On Windows 10, the Kernel file (ntoskrnl.exe) is protected and cannot be restored during a System Writer restore. Using WinBMR can and the Live CD can restore these files.
- The `restart` command has limitations with plugins, as it initiates the Job from scratch rather than continuing it. Bacula determines whether a Job is restarted or continued, but using the `restart` command will result in a new Job.

