

VTmig's General Backup Guidelines

Zeb Bowden

Version: 1.0 - 06/21/05

The VTmig backup strategy consists of using Tivoli TSM and the built-in ntbakup.exe programs. The general idea is to use TSM to start ntbakup first and then backup the entire system (including the .bkf file created by ntbakup) with TSM. This gives us the added redundancy and reliability of having two complete system backups using two different backup programs. The configuration file used for TSM is named dsm.opt and the setting used to kick off a program/batch file before the TSM backup runs is called "preschedulecmd".

Detailed system specific configurations won't be discussed in this document; you should configure your backups according to your specific needs. VTmig takes the approach to backup "everything"; this includes all of our drives and the system state on our domain controllers. The only exclusions are for files that are always in use (pagefile.sys for instance). It is critical that you backup the system state in order to restore the Active Directory database. Another thing to consider would be whether or not to encrypt your backups. VTmig uses TSM to encrypt all of our backups and have found it to work quite well. This encryption secures the traffic as well as the physical media. Proper password management is crucial when going this extra mile.

The general steps we follow and recommend are:

1. Install and configure Tivoli TSM (VTmig uses central IT's implementation, see the references section at the end of this document for more information):
 - a. Specify what you would like to backup and make sure to include the system state.
 - b. Verify that the **preschedulecmd** specification points to the ntbakup batch file discussed in step 3 below.
2. Configure ntbakup selections (.bks file):
 - a. Run ntbakup.exe
 - b. You will probably get a message about Removable Storage service not running, you can disregard this message. If you are not using the Removable Storage service you should stop and disable it.
 - c. Go to backup tab
 - d. Select the items you want to backup, for example: d, e, system state
 - e. Select job (pulldown menu), save selections as, %path_to_save_settings%\D_E_SS_ALLin1.bks (ex: e:\backups\D_E_SS_ALLin1.bks)
 - f. Close ntbakup

3. Configure the ntbakup batch file:
 - a. Create a batch file with the name and path specified above (in step 1.b)
 - b. The contents of the batch file should look similar to the following:

```
REM ntbakup of D_E_SS_ALLin1
REM the next 3 lines should actually be one long line in your batch file
%ntbackupPath% "@%bksLocation%" /n "%backupName%" /d
"%backupDescription%" /v:yes /r:yes /rs:no /hc:off /m copy /j "bu" /l:s /f
"%bkfLocation%"
```

The variables are explained below:

- %ntbackupPath% = full path to ntbakup.exe [usually c:\WINNT\system32\ntbakup.exe]
 - %bksLocation% = full path (including file name) of the .bks file [as specified in 2.e above]
 - %backupName% = the name of the backup set that will be created by this batch file [ex: Media Created on 06/01/2005]
 - %backupDescription% = the description of the backup set that will be created by this batch file [ex: Set Created on 06/01/2005]
 - %bkfLocation% = full path (including file name) of the .bkf file (i.e. the output of ntbakup) [ex: e:\backups\D_E_SS_ALLin1.bkf]
4. Test the batch file, you should be able to run it and have it produce a file (as specified by %bkfLocation%). You should be able to search for "backup*.log" to find the log file that may indicate problems with the batch file as well. The usual location of the backup log file is "Documents and Settings\<user running ntbakup>\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\data.

Steps to encrypt your backups with TSM:

1. Turn on encryption in the dsm.opt file by adding the following lines:

```
ENCRYPTKEY SAVE

include.encrypt "*/...\*"
include.encrypt systemobject
```

2. To initiate encryption and to enter the encryption password:
 - a. Use gui to backup a file that will be encrypted, so that it prompts you for the password. (Note: The encryption password, in binary format, is stored at: HKLM\SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\Nodes\<NO DENAME>\ADSM\Encrypt)
 - b. Do a full backup of your system with ntbakup.

- c. Next, perform a full backup of your system with TSM by selecting the option to “Always backup” rather than the default of “Incremental (complete)” in the TSM user interface. This will ensure that your backup files are encrypted.

IMPORTANT: Don't lose the encryption password (it is the only way to decrypt the backed up files).

Test encryption using another machine with TSM installed (assurance that file is encrypted). In this example, machine A will be the machine with encrypted backups and machine B will be the machine on which you will be decrypting and restoring the file:

- a. Copy the dsm.opt of machine A to machine B (keep a backup copy of machine B's dsm.opt file) and delete the encryptkey command as well as any inclusions / exclusions.
- b. Using the TSM Backup-Archive GUI, restore the tested file to a harmless area of machine B (it should prompt you for the password, and should not save the password in the registry if you removed the encryptkey command from the dsm.opt file)
- c. Verify that the restored file is valid and contains the expected data.
- d. Remove the modified dsm.opt file from machine B (and restore the original dsm.opt file on machine B).

References:

General Virginia Tech Backup Information:

http://www.computing.vt.edu/security_and_viruses/network_backup/

Download, install, and configure Tivoli Storage Manager (TSM) 5.2 for Windows NT/2000/XP: <http://www.answers.vt.edu/ask4help/thirdparty/vtkb1890.htm>