

# Microsoft's SBS 2003 Best Practice Guide

## For use with StorageCraft ShadowProtect

### Disclaimer

This guide is for End Users and Resellers to provide some guidance when building an SBS 2003 Server for best optimal usage of the hardware provided for the life cycle of the hardware. This document is provided in an 'as where is' basis and is based on eight years of experience.

### General Overview – criteria for a successful deployment

1. **Disable other VSS applications** (e.g. NT Backup, VCS, CDP products, etc) whilst ShadowProtect is performing VSS enabled backups. The reason for this is if two VSS applications use VSS at the same time, there is a danger of corrupting VSS. In most cases, a reboot resolves the corruption.
2. **Backup System State** (using a scheduled NT Backup job) at least once per week, outside of ShadowProtect backup times as NT Backup uses VSS.
3. **Create a backup destination that is a FIXED disk** so that retention policy works. Files and folders are then able to be restored from here. Ideally a 1TB drive should provide enough space for most SBS users. This may be a USB drive, permanently attached to the server. See archival section on page 6.
4. **VSS applications**, operating systems and databases can be backed up every 15 minutes throughout the day. Non VSS applications and databases may require the services to be stopped prior to performing the backup. This process can be scripted and automated and does not require additional agents or options
5. **When performing a hardware independent restore (HIR)** ensure that you have all the required drivers for the new server available, ideally on a USB key or on the network.
6. **If doing a physical or virtual migration** of a Domain Controller or any server with a static IP address, you must reboot in to Active Directory Restore Mode, change the IP address, then reboot again. It is also recommended to perform a full check disk and defrag after a migration – for more information, please refer to: <http://www.storagecraft.com/ServiceSupport/APACKnowledgebase/>

### Set Up

#### Partitions

For best performance and reliability for the life cycle of the server you should always partition the server disks. The reasons behind this is fragmentation of the folder and file structure with the focus on the system/boot partition being kept as small as possible to ensure reliability of the server while maintaining performance. In addition, when you are backing up or restoring it is ideal to keep data and systems in separate volumes for maximum efficiency of your backups. After the initial build have a quick look at the fragmentation and you will see that the "C:" drive

will have between 35 and 45% file fragmentation, this will affect the performance of the server. Therefore let's set the parameters for our drives:

- **“C:” Drive** – I prefer 12GB but you could go as far as 20GB and this is for the “Windows” directory plus program files.
- **“E:” Drive** – I use this for the Exchange data and the PageFile therefore choose a size that will cover the maximum size of the Exchange databases plus the PageFile. Example – this organisation will have a maximum number of users and the server has 4GB of RAM therefore this partition will be (75GB for Exchange, plus space for the log files and 8GB for the page file – this ensures that the servers' PageFile will never get fragmented because it is a single file and never cause issues with ShadowProtect backups) 100GB.
- **“F:” Drive** – is for the data plus the Client Apps folder, SharePoint, SBS Monitoring, WSUS, Home folders and Company Data and therefore needs to be 100Gb or larger.

**Summary** – this gives the best around performance with minimal maintenance and is a dream to backup and therefore restore. **Note:** Due to the restriction of restoring only to larger volumes, we recommend that you leave 2GB free at the end of disk. This helps to minimise problems when restoring to different disk manufacturers.

## Install

Start the normal install specifying the size of the system/boot partition and allow this to complete but do not allow the set up wizard to automatically logon. When you login for the next step put it on hold while you go to disk management and create your two other primary partitions of the sizes you calculated from above then format these partitions with NTFS.

1. Next go to the Computer properties, on the advanced tab click on settings under performance,
2. Next go to the advanced tab and under virtual memory click change, remove the page file from the “C:” drive and accept the warning BUT click on “SET” then click on the “E:” drive and create a custom PageFile with the initial and maximum size twice the size of the RAM installed in the server. This step ensures that the PageFile is a fixed size and will never suffer fragmentation.
3. Now allow the wizard to proceed with the Active Directory setup.
4. After the reboot the wizard continues and asks for what applications to install and here you get the choice of where to install things. Remember to install Exchange databases only into the “E:” drive into its own folder and all the rest into the “F:” drive.
5. When this is all complete install any other required applications – EG Anti Virus programs and specifically ShadowProtect – ensure that you reboot after this.

## Tuning

Remember we have dealt with the PageFile so what else do we need to fine tune; here is a simple list to ensure that we get the best performance from our system.

1. Boot.ini extensions for Exchange and on some motherboards to allow access to the entire RAM. Some of these extensions could be USERVA=3030, 4GB so investigate what is required.
2. Most importantly ensure that all Mother Board chipset drivers are installed, and that all devices are using OEM drivers where possible and not generic Microsoft drivers.
3. On the "C:" drive create a folder called TEMP, then go to system and user environment variables and point the temp and tmp locations to the new folder called C:\TEMP. The purpose of this is to store all temp files in the one location so that maintenance is easier to perform.
4. When you create schedules for your Anti Virus program ensure that full scans are performed outside of the times specified for backups as the increased disk I/O could create too much stress for VSS to cope with and it will fail thus causing the backups to fail.
5. Move the Exchange "System Path Location" (this is located in the same place where you would move the log files) for the information store from the C:\Program Files\Exchsrvr\MDBDATA folder to the location of the exchange databases on the "E:" drive. **Use System Manager to do this.**
6. This is a logical place to create a Backup folder on the "F:" Drive to store the maintenance script and the ss.bks (see the maintenance section) file. Then execute this script to perform the first disk clean up, a defrag and create your first System State Backup. Finally using Windows Scheduled tasks schedule this script to run every Saturday night.
7. The last issue to be done is to stop "Shadow Copies" from being created and to do this open Explorer and right click on the "C:" drive, select properties – Shadow Copies – **disable all shadow copies.**

## VSS

Following is a list of checks to ensure that VSS is ready to perform its job correctly.

1. Ensure that the two StorageCraft services are running.
2. At a command prompt type in **VSSADMIN LIST PROVIDERS** – it should list two, a StorageCraft and a Microsoft one.
3. Next type in **VSSADMIN LIST WRITERS** – ensure that the Exchange writer is in place, if not then modify the registry (search the web for the registry location) to turn this on and then restart the information store and check the writers again.
4. Under shares in computer management, right click and go to all tasks – configure shadow copies. Here turn off (disable) shadow copies.

## Maintenance

This section contains the script that I have always used for the disk clean up, defrag and System State backup. Please modify this script to suit your environment of your server (this same script can be used on XP, 2003 and 2003 x64 servers). **Note: This script is provided 'as is' and NOT SUPPORTED BY STORAGECRAFT**

```
@echo off
REM A script for disk maintenance and to back up system state on a server Windows 2003 or above
REM Written by Jack Alsop 1/6/2007 from Storagecraft
REM This is a great script to run on a Saturday night before you do Shadow Protect base image backups REM on
a Sunday. This script will run on XP, 2003 and 2003 x64.
REM This next section is based on removing all KB Uninstall Directories and IIS log files and all files
REM in the temp directory - in all my builds I point the System and User Environment "temp TMP" variables
REM to a folder I create on the root of the C:\ drive called temp.
Del e:\backup\list.txt
dir C:\windows\$\$* /A:DH /B >e:\backup\list.txt
FOR /F "eol=; tokens=1 " %%i in (E:\backup\list.txt) do RMDIR /S /Q C:\Windows\%%i
Del e:\backup\list.txt
del /f /Q C:\WINDOWS\kb*
del /f /Q c:\temp\*. *
del /f /q C:\WINDOWS\system32\LogFiles\W3SVC1\*. *
del /f /q C:\WINDOWS\system32\LogFiles\W3SVC****\*. *
REM This section is designed to clean up the hard disks
REM Run the following command
REM Cleanmgr.exe /d x: /sageset:zzzz ? This will start the wizard in configuration mode
REM you just need to set what you want cleaned. x: refers to the drive you want to clean
REM and zzzz: refers to any number you want to use.
REM When you run the following command insert the number you chose above - EG I used 1234
cleanmgr.exe /sagerun:1234
REM Next we do a defrag of the drives we want defrag
defrag.exe C:
defrag.exe E:
defrag.exe F:
REM Finally we backup System State by doing the following
REM Create a folder on the F: drive called "backup" (use what ever drive you want But ensure you change the
path statements below)
REM We open up NT Backup and select on the system state folder and save this selection
```

REM to the folder specific above and call the file "ss.bks" ALTERNATIVELY ask StorageCraft Australian REM for this script and we include the ss.bks file for you. NOTE this file cannot be opened with notepad REM as it will damage the file.

```
C:\WINDOWS\system32\ntbackup.exe backup "@E:\Backup\SS.bks" /n "SS" /d "SS" /n "SS" /v:no /r:no /rs:no /hc:off /m normal /j "SystemState" /l:s /f "E:\Backup\SysState.bkf"
```

REM Finally schedule this command file through Schedule Tasks for a Saturday night.

## ShadowProtect

This section covers how to set up ShadowProtect for the best result for your system.

Steps to be performed in the console

1. **Destinations** – create a destination for your backup images to be stored. This destination needs to be a FIXED disk either on the server or on some other computer/server or NAS device. Ensure that the NAS device can handle large files without breaking them up into smaller files. The fixed disk could be a USB/eSATA external device (ensure it is configured with NTFS and sleep mode is disabled) and ensure that it never gets removed otherwise the retention policies will fail. Final note here is that if the intention is to use the automatic mount scripts or incrementals forever then the NAS device cannot be used. Please ensure that the BIOS of the Image Repository is set to NEVER go in to sleep mode. It must always be connected and viewable by ShadowProtect.
2. **Automatic Mount** – ask ([support@storagecraft.com.au](mailto:support@storagecraft.com.au)) for the zip package and extract into the C:\Program Files\StorageCraft\ShadowProtect\ folder. Read the attached document and create the restore folders then modify the scripts to suit your environment and using the logon script create an “R:” drive that maps the restore folder above to this “R:” drive for all users. **Note:** This is provided ‘as is’ and NOT supported by StorageCraft.
3. **Create jobs** – for most customers the weekly schedule is the best choice and therefore the rest of this section will refer to this backup selection. To obtain the best result create separate jobs for each partition/drive. Therefore lets create a job selecting the “C:” drive – when we get to the schedule section create a base on a Sunday Morning and then incrementals Monday to Friday but because of our setup of the server we only need to do 3 incrementals per day. The next step is to password protect our images (**Caution:** record this password somewhere as there is no back door) and then in the advanced tab go to the retention policy and select 2 images but select the check box to delete the base and incrementals. Finally finish the wizard and execute. The “E:” drive is next and we will do as above with a few minor differences – ensure that the base time creation is a least 30 minutes later with the incrementals starting 10 minutes after the start time for the “C:” drive – secondly the incrementals for this partition should be done every 15 minutes (you choose what you feel is best for your clients) – remember the retention policy. The last drive, the “F:” drive will be done as per the “E:” drive but start the base 30 minutes (or when you estimate the “E” drive to complete its full backup) after the “E:” drive with the incrementals 10

minutes after the “E:” drive – don’t forget the retention policy. Finally, if you chose to use the automatic mount script, in the post backup command point to the mount.cmd mentioned in point 2 above.

4. **System State Backups** – it is essential that you backup System State at least once per week using a scheduled NT Backup job. This job should run outside of the ShadowProtect backups as NT Backup also uses VSS and you should not run two VSS applications at the same time.
5. **Final task – archive of your images** – most people today are using USB drives for the removal offsite of the images, therefore as a post backup command for the “E:” drive I suggest a RoboCopy script that copies from your Fixed disk to the USB take home drives. This script is as simple as “robocopy.exe H:\images I:\images /COPY:DAT /E /V /PURGE /ZB”. Cut and paste this into notepad and save it into C:\Program Files\StorageCraft\ShadowProtect\ folder as backup.txt then rename to backup.cmd and by editing the “E:” job in the advanced tab – under commands add this as a post backup command. This way your removable USB drives will always be a true copy of your fixed drive. Caution, ensure that you copy RoboCopy.exe into the C:\Windows\System32 directory.
6. **Test and Verify** – It is **STRONGLY** recommended that after the first full backup of each volume that you immediately instigate three incremental backups (right click on the backup job) one after each other on all volumes protected by ShadowProtect – they should only take a couple of seconds each. Once finished, mount each volume (using the third option <**Explore Backup**> from the main menu) to ensure that the images are completed and able to be mounted. Test the entire backup set at least once per week.

## Other Information

StorageCraft is committed to providing an outstanding level of support to our customers and partners. Customers should be covered by a current maintenance agreement prior to contacting technical support. In Asia Pacific, the regional (Sydney based) technical support team can be contacted by various methods:

- **On-line Knowledgebase:** <http://www.storagecraft.com/ServiceSupport/APACKnowledgebase/> - we have developed an on-line support portal for customers and resellers to enable them to self-help themselves and resolve their own issues. It is recommended that customers try the knowledgebase portal or the StorageCraft Forum (see below) prior to submitting a support request.
- **On-Line Forum:** <http://forum.storagecraft.com/Community/forums/> this is a valuable forum to view questions and their solutions from other customers. New issues or questions can be registered here.
- **E-mail:** [support@storagecraft.com.au](mailto:support@storagecraft.com.au) – please ensure you include all your company details and a detailed summary of the problem and log files if possible when e-mailing the technical support team.
- **Asia Pacific Telephone Support:** + 61 2 9929 9770 (Sydney, Australia)
- **Flash Demonstration (15 minute duration):** [http://www.storagecraft.com/ProductTours/ShadowProtect\\_demo.asf](http://www.storagecraft.com/ProductTours/ShadowProtect_demo.asf)
- **VMware Flash Demonstration (2 minute duration):**  
[http://www.storagecraft.com/ProductTours/ShadowProtect\\_VMware\\_Workstation.asf](http://www.storagecraft.com/ProductTours/ShadowProtect_VMware_Workstation.asf)