STORAGECRAFT. SHADOWPROTECT 4

BEST PRACTICES GUIDE

Configuring ShadowProtect and Windows

13 July 2012 • Revision 2

POWERED BY STORAGECRAFT Technology Corporation

Document ID:	BP000009
Revision:	2
Date:	13 July 2012
Author(s):	Jack Alsop StorageCraft Asia Pacific

For Technical Support contact your regional office:

North America

StorageCraft Technology Corporation
11850 South Election Road, Suite 120
Draper, Utah 84020
USA

w forum.storagecraft.com/Community/web2case/
w www.storagecraft.com

Asia Pacific

StorageCraft Pty Ltd
Level 11, 53 Walker Street
North Sydney NSW 2060
Australia

w forum.storagecraft.com/Community/web2case/
w www.storagecraft.com.au

Europe

StorageCraft Europe AG
Oberneuhofstrasse 5
CH-6340 Baar

w forum.storagecraft.com/Community/web2case/
w www.storagecraft.eu

Table of Contents

Synopsis 5
Configuring Windows for a successful ShadowProtect deployment 5
System volumes 5
Use complete disks 6
Hardware RAID 6
Host SATA RAID 6
Disk Queue lengths 7
Paging files 7
Volume Shadow Copy Service (VSS) 7
Windows Scheduled Tasks 8
Disk defrag 8
Understand your data 8
One volume per job 8
Configuring ShadowProtect for ultra-reliable business continuity 8
Thou shalt 8
SPDIAGNOSTIC 9
Full or custom install? 9
Image repository 9
Create destinations 9
Agent options 10
Configuring a backup job 10
Complementary products 11
References 12
Products affected 12
Platforms affected 12
Replaces article 12
Supplemental articles 12

Synopsis

This Best Practices Guide will cover configuring ShadowProtect and Windows to achieve maximum performance and results in your deployments.

Configuring Windows for a successful ShadowProtect deployment

Here are some tips on configuring your Windows operating system to deliver improved performance and enable ShadowProtect to operate optimally.

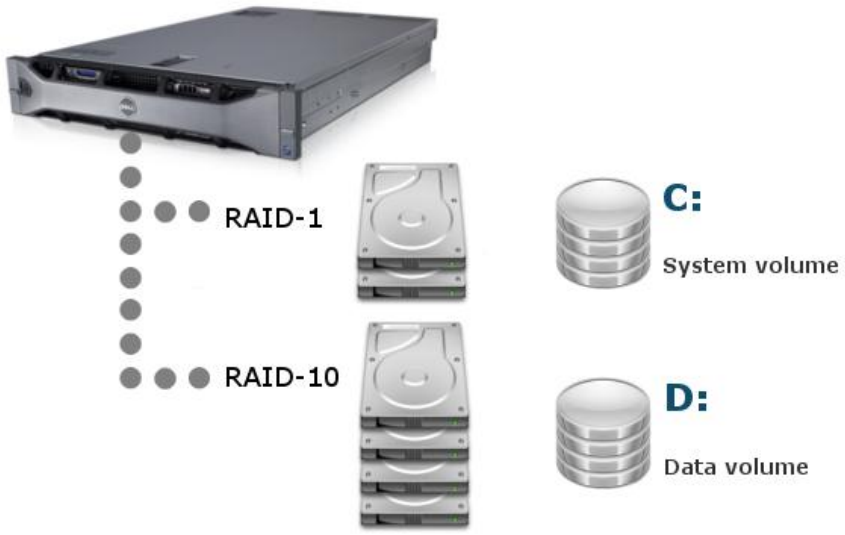

Figure 1: Server configuration (optimal)

System volumes

System volumes should be on small, fast, high performance disk drives, and ideally for Windows Server 2008 R2, the system volume should be 60-100 GB in capacity. Large system volumes have a detrimental effect on performance and recoverability caused by Windows disk fragmentation. Disk fragmentation causes the biggest performance degradation to Windows environments.

A system volume should contain only the operating system and application binaries. No application data (or user data for that matter) should reside here; that is what data volumes are for.

Use complete disks

Where possible, only use whole disks as partitioned disks can impact server performance.

This is crucial for the System partition. If your current configuration does not allow this, then a large disk partitioned into a small system partition and a data partition (refer to Figure 2) is still better than one large system volume.

Figure 2: Server configuration (alternate)

Hardware RAID

For system volumes, use hardware mirrored RAID (RAID-1) based on business grade SAS or SATA disks.

For your data volumes use hardware RAID-10 as this will provide the best performance for your applications and data.

Host SATA RAID

Do not use host SATA RAID (which in reality is nothing more than software RAID) as it has performance implications due to the fact that there is no separate dedicated CPU to perform the processing, and therefore is not recommended on any production server.

Disk Queue lengths

By running Performance Monitor and selecting the *Average Disk Queue Length* counter from the *Physical Disk* performance object for the volume you want to monitor, you can get a good idea of the disk sub-system load.

The basic recommended formula is:

```
n = (Average Disk Queue Length value) – (number of disks in array)
```

n should be less than two. If *n* is greater than two, then the disk sub-system is loaded to capacity. If *n* is less than two then there should be no need for concern.

Paging files

Use fixed size paging files. The recommended size for paging files is twice physical memory for file servers and four times physical memory for application servers such as Microsoft SQL and Microsoft Exchange. If the server has 32 GB or more of physical memory, then use twice physical memory for application servers.

This reduces disk fragmentation as the page file should always be a contiguous file which improves I/O performance.

A more technically correct solution is to follow Microsoft's Mark Russinovich's technical document (http://blogs.technet.com/b/markrussinovich/archive/2008/11/17/3155406.aspx) that describes the setting as "find your Peak Commit – Physical RAM, and then set the minimum and maximum to double that figure but remember that you will need at least 1 GB if you want crash dumps".

The final point is, where possible put the paging file on its own partition but regardless get it off the system volume as this is the busiest volume on your system.

Volume Shadow Copy Service (VSS)

Never, ever have two applications call VSS at the same time. Never perform a "Previous Versions Snapshot" (which by default occur at 0700 and 1200 hours daily) and a ShadowProtect backup at the same time as it will potentially corrupt and/or damage the VSS infrastructure. Know what existing SQL maintenance plans are in place and perform ShadowProtect backups outside of these times.

ShadowProtect uses the VSS framework to freeze and thaw data. Data and most databases (for example Microsoft's Exchange, SQL and SharePoint and Oracle etc) can be backed up every 15 minutes.

StorageCraft has developed an application called VDIFF which is a combination of a very low level Disk I/O Kernel driver and a bitmap stored in kernel memory. VDIFF has only one purpose which is to track and record disk changes at the sector level. This feature results in ShadowProtect being the fastest snapshot technology available on the market because it does not need to interrogate the MFT (Master File Table) to identify what sectors have changed since the last backup.

The MFT is still queried once during a snapshot to establish if the MFT is clean or dirty. If it is dirty, ShadowProtect will deliberately fail the next incremental so that corrupt data is not backed up.

Windows Scheduled Tasks

There are some 35 scheduled tasks configured on a Windows Server 2008 R2 server, with approximately 25 active tasks.

All of these are scheduled to run on the hour. For this reason, never run ShadowProtect on the hour; start backups two to three minutes after the hour. For example, schedule the backup to commence at 0703 hours rather than 0700 hours.

Disk defrag

To maintain system performance, schedule disk defrags on a regular basis. Ideally, once per week but always schedule after business hours. Note that on Windows Server 2008 and higher, a disk defrag is automatically scheduled for 0100 hours every Wednesday.

Also be aware that the next incremental backup after a disk defrag will be larger than normal.

Understand your data

Understand your server and your data. Often there is data on production servers that never needs to be backed up.

The two most common components in this category are anti-virus software and Windows Server Update Services (WSUS). These two components should be performed as custom installs into a separate partition (ideally on a disk that does not contain the system volume) that is only ever backed up once before these applications can initially update themselves and never back them up again as it is not critical data and not required for a server recovery.

Note: not all anti-virus programs integrate well with Windows as some of them use the `ProgramData` directory in the system volume to store their updates. This will often cause at least one 4 GB incremental backup per day.

One volume per job

Ensure that your applications are configured to support our best practice recommendation of only backing up one volume per job where possible.

Please see the Microsoft Exchange Server 2003/2007 Best Practice Guide for an explanation on how to achieve this. This article can be seen at http://www.storagecraft.com.au/best-practice-guides/BP000002%20Microsoft%20Exchange%20Server%202003-2007.pdf.

Configuring ShadowProtect for ultra-reliable business continuity

Spending approximately 2-5 minutes per server during the configuration phase will save you hours of time during the management phase.

Attend our technical training courses or watch our online videos, or contact StorageCraft Sales directly to better understand our technology and the solution we provide.

Thou shalt

Reboot a server before installing ShadowProtect. This helps to ensure that any applications or Windows Updates are applied before ShadowProtect is installed, and that the server is bootable.

SPDIAGNOSTIC

Download SPDIAGNOSTIC from ftp://ftp.storagecraft.com.au/tools/ (you can select from a ZIP or self-extracting executable) and run this in Pre-Install mode to see if in fact your server is ready for the installation of ShadowProtect.

If this utility finds any issues then it will report at the bottom of the document the knowledge base articles that reference your issues. Please address these issues and then reboot before installing ShadowProtect.

Full or custom install?

There are two installation types available.

Full install

A full install includes the console, backup agent, snapshot provider and driver, mount tools and VirtualBoot.

Custom install

A custom install allows you to select from the components to install. Typically you will use a custom install when setting up a management workstation or a disaster recovery server with VirtualBoot and Oracle VirtualBox when the backup agent (which requires a license) is not required.

Regardless of the installation type selected, reboot immediately after installing.

Image repository

On your fixed image repository or Disaster Recovery appliance, create sub-folders under a common shared folder for each server to be backed up using the same naming convention as your production servers.

For example, if your Microsoft Exchange server is called AUSMAIL01, then create a sub-folder called AUSMAIL01 and then this sub-folder is where all the backups for this server's volumes will be written.

This will avoid any future confusion of which images belong to what server. Having your image repository configured in this way will also be beneficial if you choose to use any of the enterprise ImageManager features such as Intelligent FTP and HeadStart Restore.

Note: If you have Continuous Incremental and normal Weekly Full and Incremental backup types on the same server, ensure that images from both backup types are not stored in the same sub-folder. Separate the two backup job types into separate folders again.

Create destinations

Within the ShadowProtect console, always create backup destinations first before configuring any jobs. Remember that if it is a remote connection then use an account that has the correct permissions.

We strongly recommend that you create a Windows service account that is a Domain Administrator with a very complex password that only changes once a year. This account should not be used for daily administrative tasks.

Agent options

Set up the agent options and licence the agent.

Most of the agent options are about email alerts and to get them right, please refer to http://www.storagecraft.com/support/sites/support.storagecraft.com/files/old/00000191%20Configuration%20of%20Email%20Options.pdf for configuration and suggestions.

Configuring a backup job

For this exercise, we will assume that our theoretical file and print server (Figure 1) has three volumes and we will be using continuous incremental jobs.

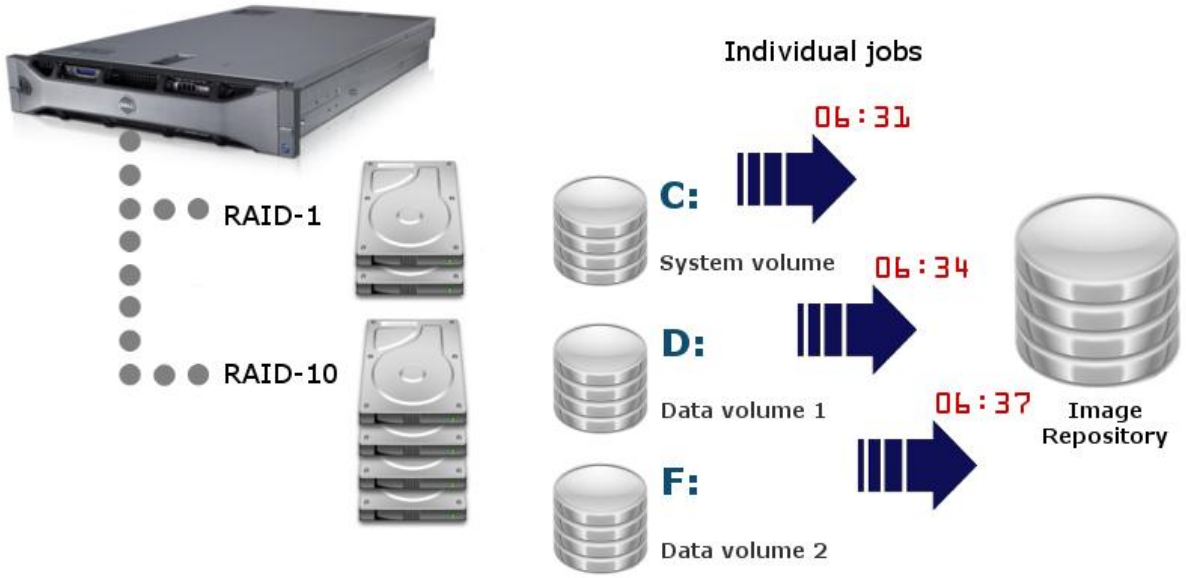

Figure 3: File and print server

System volume

The system volume needs to backed up at least three times per day. If it is a Domain Controller and SYSVOL and NTDS are stored on the system volume, then we should back this volume up at least five times per day. Remember when backing up a Domain Controller with ShadowProtect you are also performing a System State Backup.

The working day for this server, based on the demands of the company, is from 7.00 AM to 7.00 PM. Therefore we will start the daily incrementals at 6.31 AM (0631 hours) and finish at 7.31 PM (1931 hours).

Data volume 1

Staggering the start times, data volume 1 will start its daily incrementals at 6.34 AM (0634 hours) and finish at 7.34 PM (1934 hours). The backup interval will typically be 30-60 minutes depending on business need and data residing on the volume.

Data volume 2

Again, staggering the start times, data volume 2 will start its daily incrementals at 6.37 AM (0637 hours) and finish at 7.37 PM (1937 hours). The backup interval will typically be 30-60 minutes depending on business need and data residing on the volume.

Notes

Some points to take note of.

If there is a remote chance that these backup files can be accessed by any unauthorised personnel then password protect the backup images. Ensure that you record the password as there is no back door for lost passwords. Using password protection also enables data encryption (up to 256-bit).

Do not give these backup files a long name as sooner or later Windows will not be able to mount the backup chain because the path to the images will be too long.

When performing the initial full backups on the server, start the system volume backup first and then when it completes, start the backup of data volume 1 and so on to prevent the server from becoming overloaded.

Complementary products

To complete your installation, there are a couple of complementary products that we recommend. Consider using ShadowControl ImageManager and WatchDog for the added confidence that your backups are in good shape and tested for recoverability.

References

Products affected

- StorageCraft ShadowProtect

Platforms affected

- All

Replaces article

Supplemental articles

BP000002 Microsoft Exchange Server 2003/2007

00000191 Configuration of Email Options

NOTES:

2012/BP000009:2