

# SharePoint Disaster Recovery Options



**Sean P. McDonough**  
Product Manager, SharePoint Products  
Idera

# What we'll cover



- Understand backup targets
- Define the SharePoint targets
- Examine common related targets
- Discuss a few esoteric targets and edge case scenarios
- Wrap it all up

# Target talk

- What is a target?
  - Targets are the “what”
  - They can be protected
  - Tangible – typically file(s)
  - Can be described and referenced in a plan
  - Prioritized for protection & recovery
- Many different target types
  - Some targets are common
  - Other targets vary by farm purpose and platform technologies in-use



# Target talk

- Our focus: the technical (DR plan) targets
  - What are they?
  - Where do they reside?
  - When are they important?
  - Protection approaches\*
  - Special considerations and watch-outs
- Remember
  - Today's focus is on the technical, but ...
  - Targets should be driven by business



# SharePoint targets



- Content DBs
- Central admin DB
- Farm config DB
- SSPs and service applications
- Search

# Content databases

- Hands-down #1 target set
  - Houses the majority of your users' content
  - Must protect; can't be recreated if lost
- Where are they?
  - SQL Server (all those **wss\_** databases)
  - At least one database per Web application
- Protection
  - (SharePoint) farm backups, SQL backups, high availability (HA) mechanisms, 3<sup>rd</sup> party tools
- Watch-outs: RBS pointers



# Central admin content database

- What is it?
  - Simply another content database
  - Houses Central Administration site collection
  - Usually 1<sup>st</sup> content DB with a GUID
  - Each farm gets its own when the farm is first created
- Worth protecting?
  - Usually not\*



# Farm configuration database

- What is it?
  - Repository for farm-wide configuration data, web application settings, services information, and more
- Worth protecting?
  - With SP2007, generally not; with SP2010, usually yes!
- Where is it?
  - SQL Server (`SharePoint_Config`)
- Protection
  - Farm backups, SQL backups, HA
  - mechanisms, 3<sup>rd</sup> party tools, documentation<sup>1</sup>



# SSPs and service applications

- What are they?
  - A collection of services (Excel services, BDC, Managed Metadata, etc.) that are consumed by Web applications and their site collections
- Worth protecting?
  - Yes for both SSPs and the majority of service applications
- Where are they?
  - Simple answer: all over the place ...



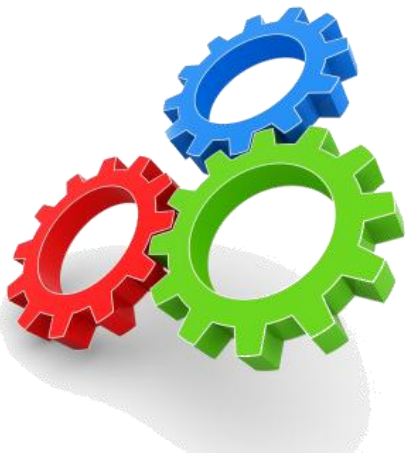
# SSPs and service applications

- No really – where are they?

- Many have one or more databases
- All have (farm) configuration data
- Most are backed by Windows services
- Service applications also have proxies
- Many differences from service to service

- Protection

- Recommended: protect as part of a farm backup (ideal) or categorically (e.g., SSP backup)
- Optionally: protect databases and augment with documentation of settings and config



# SSPs and service applications

## ■ Watch-outs

- Service applications are complex and more than just a database to back up
- Some services and service applications rely on external data that does not get included in “standard” backups; e.g., Single Sign-On service (2007) and the Secure Store Service application (2010)
- Protection guidelines vary from service (app) to service (app)



# Search



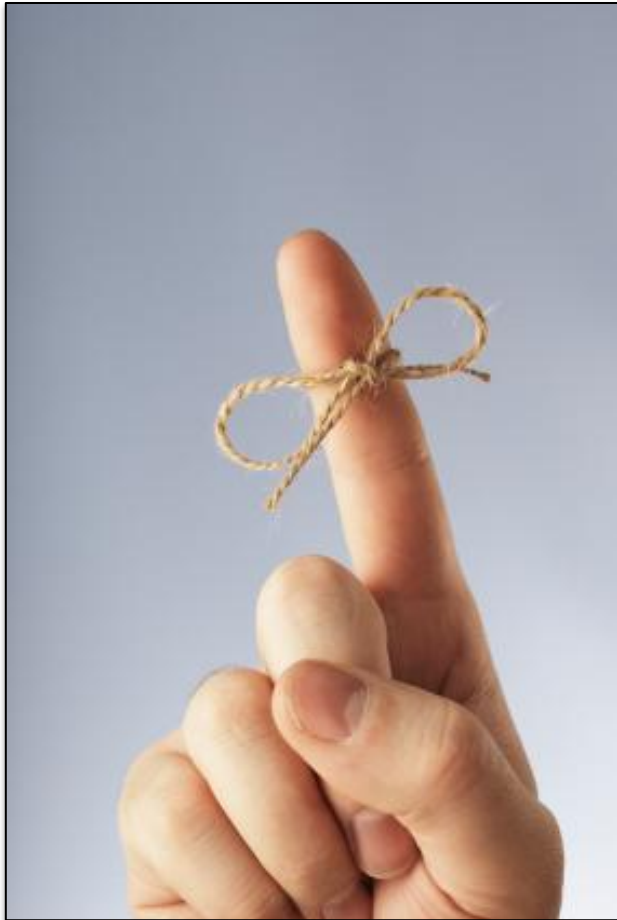
## ■ What is it?

- A combination of databases and file system data used for search crawling, querying, and administration
- Search is a somewhat special case of an SSP function/service application

## ■ Watch-outs

- Backup synchronization of index partitions & crawl database is critical
- Use either platform backup or a tool that engages the SPF-VSS Writer<sup>2</sup>

# Related targets



- Solution packages
- SharePoint Root
- IIS configuration
- Certificates
- IIS web root
- GAC
- Registry
- Bits and bytes

# Solution packages

## ■ What are they?

- .wsp files that are added to the farm to deploy custom code, Features, and capabilities
- You are packaging your customizations and custom code this way ... right?

## ■ Worth protecting?

- Absolutely. In many cases, backup is critical

## ■ Protection

- Varies (Centrally managed vs. decentralized)<sup>3</sup>
- Basic file protection/backup
- SP2010 provides configuration-only backup<sup>4</sup>



# SharePoint Root



- What is it?
  - The guts of SharePoint's core file system
  - Also known as the 12-hive or SharePoint Root
- Where is it?
  - `C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14 (or \12)`
- Worth protecting?
  - Depends on Feature and customization usage
- Protection
  - File system backup

# IIS configuration

- What is it?
  - Settings used to serve web pages by IIS
  - Covers app pools, ports, protocols, etc.
- Where is it?
  - `C:\Windows\system32\inetsrv` by default (IIS6 Metabase and IIS7.x config)
- Worth protecting?
  - Some of it, but redundancy w/ SharePoint exists
- Protection
  - File copy\*, `appcmd.exe`\*, documentation



# Certificates

- What are they?
  - In most cases, support for SSL sites via HTTPS
- Where are they?
  - Certificate store (accessible via Certificates MMC snap-in)
- Worth protecting?
  - Yes
- Protection
  - Export from Certificates snap-in or IIS Manager as **.PFX** files
  - One time operation (until cert renewal)



# IIS web root (for SharePoint)

## ■ What is it?

- Web files for each IIS site associated with a SharePoint Web application

## ■ Where is it?

- `C:\inetpub\wwwroot\wss\VirtualDirectories`

## ■ Worth protecting?

- Usually yes (`web.config` files, web part files\*, etc)

## ■ Protection

- File system backup, documentation



# GAC

- What is it?
  - The Microsoft .NET Framework Global Assembly Cache
  - Repository for shared libraries and native images
- Where it it?
  - By default, `C:\Windows\assembly`
- Worth protecting?
  - Sometimes (typically for decentralized customizations)
- Protection
  - File system backup\*

# Registry



- What is it?
  - Windows (OS) database for program info
- Where is it?
  - `C:\Windows (System.dat, User.dat)`
  - Usually accessed via tool (`regedit.exe`)
- Worth protecting?
  - Yes for some branches (`HKLM\SOFTWARE\Microsoft\Office Server\14.0\...`)
- Protection
  - `Regedit.exe` export, documentation

# Bits and bytes

- **What are they?**
  - The (often-forgotten) files and installers you need to rebuild a SharePoint environment
  - SharePoint setup files, OWAs, SPs, CUs, iFilter packs, SQL client install, etc.
- **Worth protecting?**
  - If your strategy involves rebuilding a SharePoint farm, it's well worth the time
- **Protection**
  - External media/disks, replicated storage



# Edge cases & esoteric targets

- .NET Framework config folders
- Remote BLOB storage (RBS)
- SQL Server transparent data encryption (TDE)
- External data sources



# .NET Framework config folders

- What are they?
  - System-wide configuration files and defaults in the .NET Framework installation folders
- Where are they?
  - `C:\Windows\Microsoft.NET\Framework\v...\Config`
  - `C:\Windows\Microsoft.NET\Framework64\v...\Config`
- Worth protecting?
  - Yes if you've altered `machine.config` or similar files
- Protection
  - File system backup, documentation

# Remote BLOB storage

- What is it?
  - Alternate location where BLOBs are stored when RBS is in-use<sup>5</sup>
- Where is it?
  - Varies and depends on RBS provider
- Worth protecting?
  - Absolutely critical if you use RBS
- Protection
  - Varies; consult RBS provider guidance



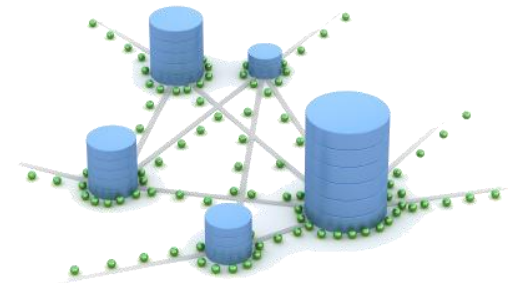
# SQL Server TDE



- What is it?
  - TDE = Transparent Data Encryption<sup>6</sup>
  - Real-time encryption/decryption of SQL Server data and log files
- Where is it?
  - SQL Server (master DB or EKM module)
- Worth protecting?
  - Certificate + key protection is critical for TDE
- Protection
  - Export followed by file backup is common

# External data sources

- What is it?
  - Data that is consumed by SharePoint but resident elsewhere
- Where is it?
  - Examples include BCS external data sources and SQL Server Reporting Services databases
- Worth protecting?
  - Highly variable
- Protection
  - Varies by data source and platform



# Wrap-up

- **Your targets are unique to your farm**
  - Understand how your SharePoint environment is used
  - Use cases are a good starting point for technical targets
- **There's more than one protection strategy**
  - Realistically, not everything has to be backed-up
  - Documentation can be a viable choice in some cases
- **Protect your (content) databases!**
  - Most important targets in your farm
  - Critical protection takes minutes. Just invest a little time<sup>8</sup>

# References

1. “Document farm configuration settings (SharePoint Server 2010)”
  - <http://tinyurl.com/SPDRFarmDoc2010>
2. “Overview of SharePoint Foundation and the Volume Shadow Copy Service”
  - <http://msdn.microsoft.com/en-us/library/cc264314.aspx>
3. “Back up and restore customizations (Windows SharePoint Services)”
  - [http://technet.microsoft.com/en-us/library/ee216349\(office.12\).aspx](http://technet.microsoft.com/en-us/library/ee216349(office.12).aspx)
4. “Configuration-Only Backup and Restore in SharePoint 2010”
  - <http://sharepointinterface.com/2010/09/10/configuration-only-backup-and-restore-in-sharepoint-2010/>
5. “Overview of Remote BLOB Storage (SharePoint Foundation 2010)”
  - <http://technet.microsoft.com/en-us/library/ee748607.aspx>

# References

6. “Understanding Transparent Data Encryption (TDE)”
  - <http://msdn.microsoft.com/en-us/library/bb934049.aspx>
7. “Plan for backup and recovery (SharePoint Server 2010)”
  - <http://technet.microsoft.com/en-us/library/cc261687.aspx>
8. “Scheduling SQL backups for SharePoint”
  - <http://www.toddklindt.com/blog/Lists/Posts/Post.aspx?ID=248>

# Additional SharePoint Resources

- Your local user group (COSPUUG)  
(<http://www.cospug.com>)
- SharePoint Saturdays  
(<http://www.SharePointSaturday.org>)
- Secrets Of SharePoint  
(<http://www.secretsofsharepoint.com>)
- Twitter  
[@SharePointTip](https://twitter.com/SharePointTip)

# Finding me

## Sean P. McDonough

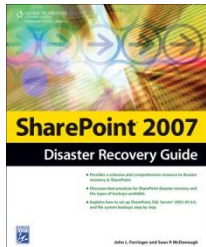


Blog: <http://SharePointInterface.com>

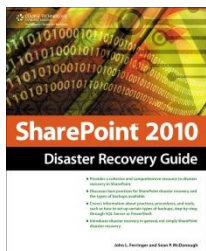
Email: [sean@SharePointInterface.com](mailto:sean@SharePointInterface.com) or  
[sean.mcdonough@idera.com](mailto:sean.mcdonough@idera.com)

LinkedIn: <http://www.linkedin.com/in/smcdonough>

Twitter: [@spmcdonough](https://twitter.com/spmcdonough)



**The SharePoint 2007 Disaster Recovery Guide**  
<http://tinyurl.com/SPDRGuide2007>



**The SharePoint 2010 Disaster Recovery Guide**  
<http://tinyurl.com/SPDRGuide2010>