SharePoint Cincy

March 16, 2012

Selecting & Protecting the Right SharePoint Backup Targets

Sean P. McDonough

- Open wireless access is available.
- Feel free to Tweet (#SPcincy2012) and blog during the session.

I'm @spmcdonough on Twitter

Thanks to our Title & Platinum Sponsors

Microsoft

cai
CENTER FOR APPLIED INFORMATICS
NORTHERN KENTUCKY UNIVERSITY

ascendum
Rise Together

MAX
max technical training

SOGETI

K2

#SPcincy2012 on Twitter
www.sharepointcincy.com

Selecting and Protecting the Right SharePoint Backup Targets

Sean McDonough
Chief SharePoint Evangelist
Idera

What we'll cover

What we'll cover

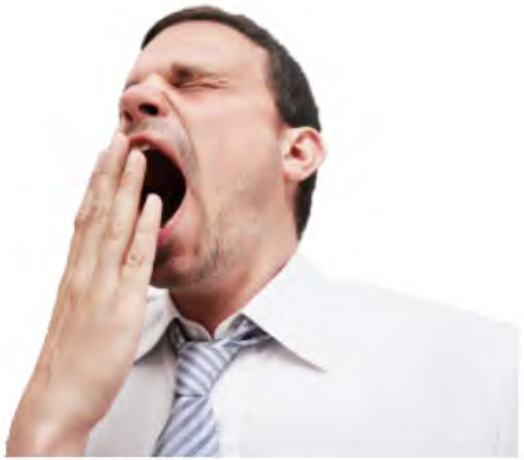
- Define a backup target
- Identify the SharePoint targets
- Examine related backup targets
- Discuss a few esoteric targets and edge case scenarios
- Wrap it all up

but first …

Why am I talking about disaster recovery (DR)?

Why am I talking about disaster recovery (DR)?

- I was a DR architect for a Cincinnati-based financial services and insurance company
- I've co-authored two books on SharePoint disaster recovery
- I'm fascinated by the sight of people yawning.



I'll do my best to
keep it interesting ...

... without getting
too crazy.

DR

"How" vs "What"

"How" w

How to set up a DR farm or warm site

How to perform a backup and restore

How to establish high availability

"How" is about tools and procedures

s "What"

What you should be protecting

What the viable strategies are for a target

What makes a target unique

"What" is all about backup targets

t backup targets

- They can be protected
- Tangible – typically file(s)
- Can be described and referenced in a plan
- Prioritized for protection and recovery

Different target types

- Some are common in all SharePoint environments
- Others vary by farm purpose or by platform technologies in-use

Two different pictures of backup targets

Two different pictures

BCP* Picture

- This is how business stakeholders see targets
- Focuses primarily on use cases tied to business activities and data
- Somewhat abstract and less concretely defined

E
c
c

Example: "Systems for inventory tracking and control must be restored"

BCP = business continuity plan

BCP*

DR Plan Picture

- Fits within the BCP
- Typically focuses on the platforms & technologies needed by business
- Targets typically defined more concretely than within the BCP

...d"

Example: "The 'Inventory' site collection, Excel services, and BCS connections to SAP must be restored"

Two different pictures of backup targets

BCP* Picture

- This is how business stakeholders see targets
- Focuses primarily on use cases tied to business activities and data
- Somewhat abstract and less concretely defined

DR Plan Picture

- Fits within the BCP
- Typically focuses on the platforms & technologies needed by business
- Targets typically defined more concretely than within the BCP

Example: "Systems for inventory tracking and control must be restored"

Example: "The 'Inventory' site collection, Excel services, and BCS connections to SAP must be restored"

Our focus today

Our focus today

The technical (DR plan) targets

- What are they?
- Where do they reside?
- When are they important?
- Protection approaches*
- Special considerations and watch-outs

I

r

Eve
foc
the
pric
be

ıı/ targets

?

Important reminder:

Even though this presentation focuses on technical targets, the actual selection and prioritization of targets should be driven by the business.

DR plan

Business continuity strategy

DR Horizon

what we'll cover in this session ...

Core SharePoint targets

aka, "the meat and potatoes"

- Content databases
- Central Admin (content) DB
- Farm Configuration database
- Service Applications / SSPs
- Search

Related targets

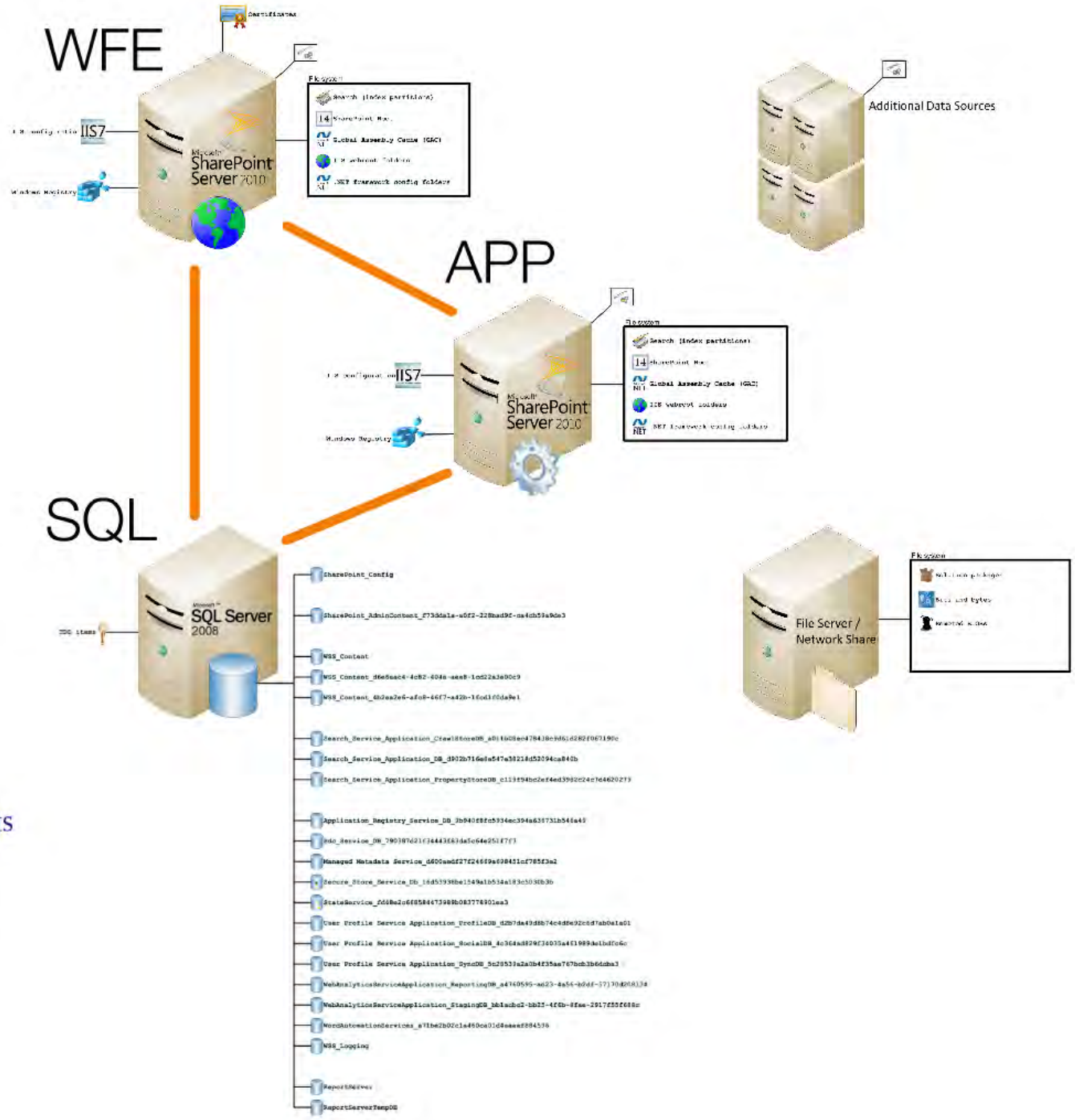
"important to remember"

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

Edge cases and esoteric targets

sometimes confused with the dark arts ...

- .NET framework config folders
- Remote BLOB storage (RBS)
- SQL Server TDE
- External data sources
- Single server farm ...



Core SharePoint targets

aka, "the meat and potatoes"

- Content databases
- Central Admin (content) DB
- Farm Configuration database
- Service Applications / SSPs
- Search

Content databases

- Hands-down #1 protection target set
- Houses 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, 3rd party tools

Watch out for RBS ...

Central Admin content DB

- Simply another content database
- Houses Central Admininstration site and help collection

Where is it?

- SQL Server
- Usually 1st content DB with a GUID

Protection

- Farm provisioning creates a new one
- Not usually worth protecting*

Farm Configuration DB

- Repository for farm-wide configuration data, web application settings, services information, and more

Where is it?

- SQL Server
- Called SharePoint_Config by default

Protection

- Worth protecting? Well, that depends ...

Protection

- Worth protecting? Well,

2007 vs 2010

2007

Not portable or supported for stand-alone restore, so backup value is questionable

2010

Still not portable or supported for stand-alone restore, but configuration backup/restore is now possible in 2010!

Protection

- Worth protecting? Well, that depends ...

2007 vs 2010

Not portable or supported for stand-alone restore, so backup value is questionable

Now that I've said that ...

Still not portable or supported for stand-alone restore, but configuration backup/restore is now possible in 2010!

Protection options

options

- SharePoint backups
- SQL Server backups
- HA mechanisms
- Documentation
- 3rd party tools

- 3rd party tools

Service Applications (2010)
Shared Service Providers (2007)

- A collection of services that are consumed by Web applications and their site collections

  Excel services, Managed Metadata Service, BDC/BCS, User Profile Service, etc.

Worth protecting?

- For both SSPs and the majority of service applications, the answer is "yes."

Where are they?

- Simple answer: all over the place ...

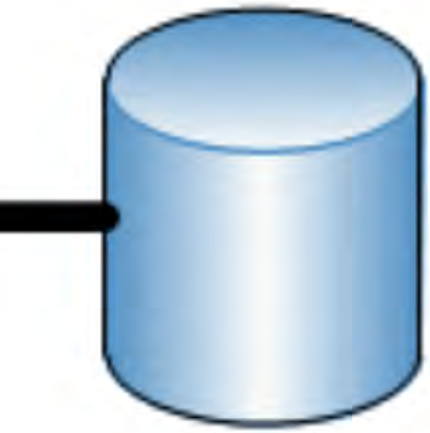
Protecting them

- Farm backup (ideal)
- Categorically (e.g., SSP backup)
- 3rd party tools

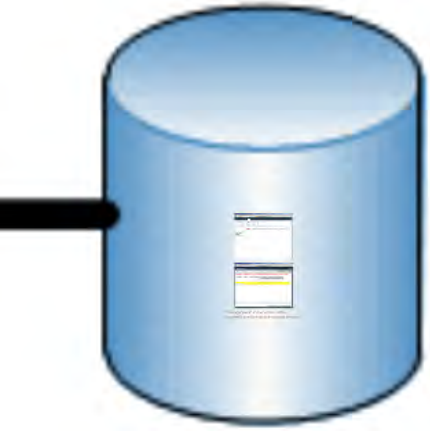
or

- Protect databases and augment with documentation of config/settings

Watch out for omitted config items and required external data. For example ...

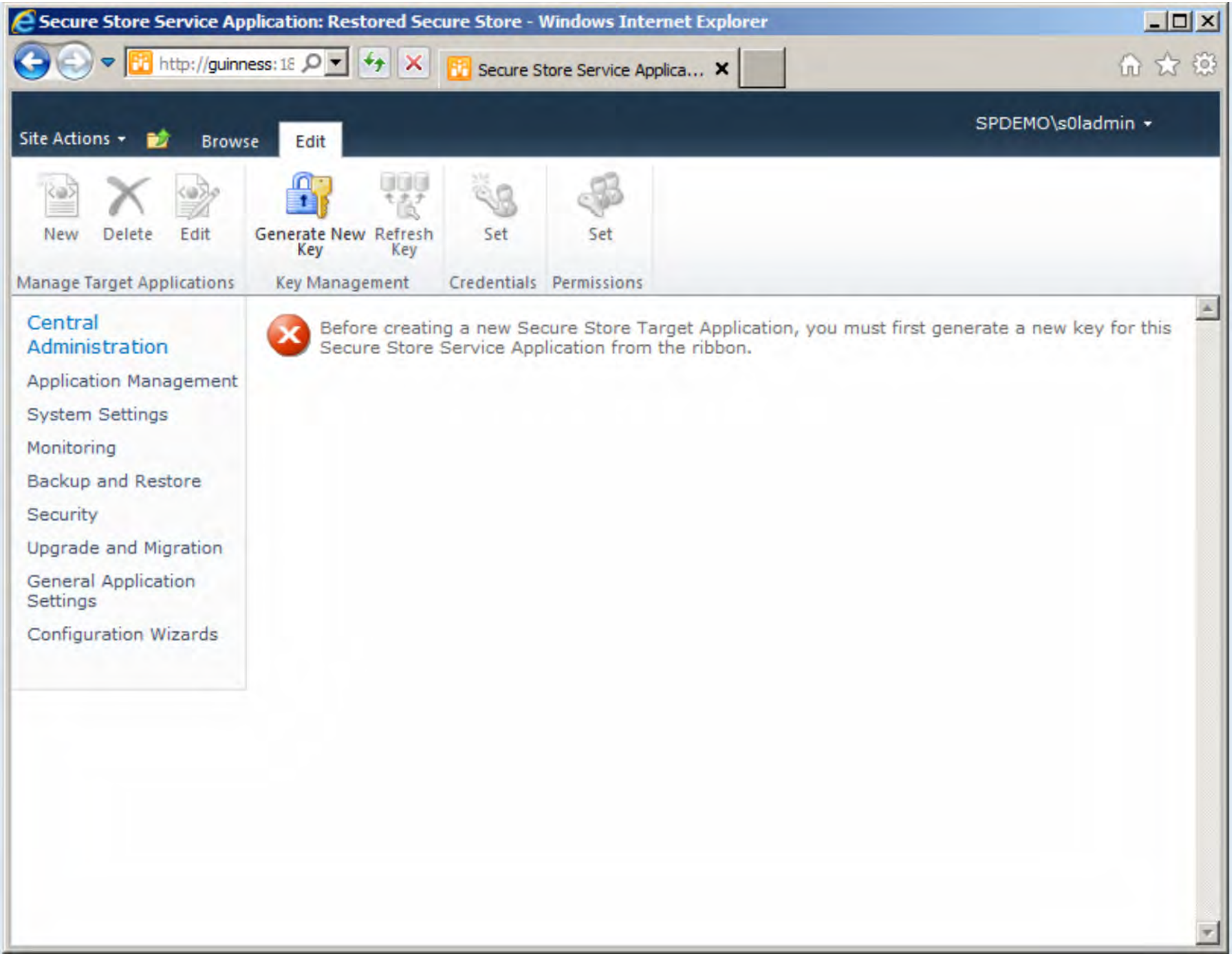


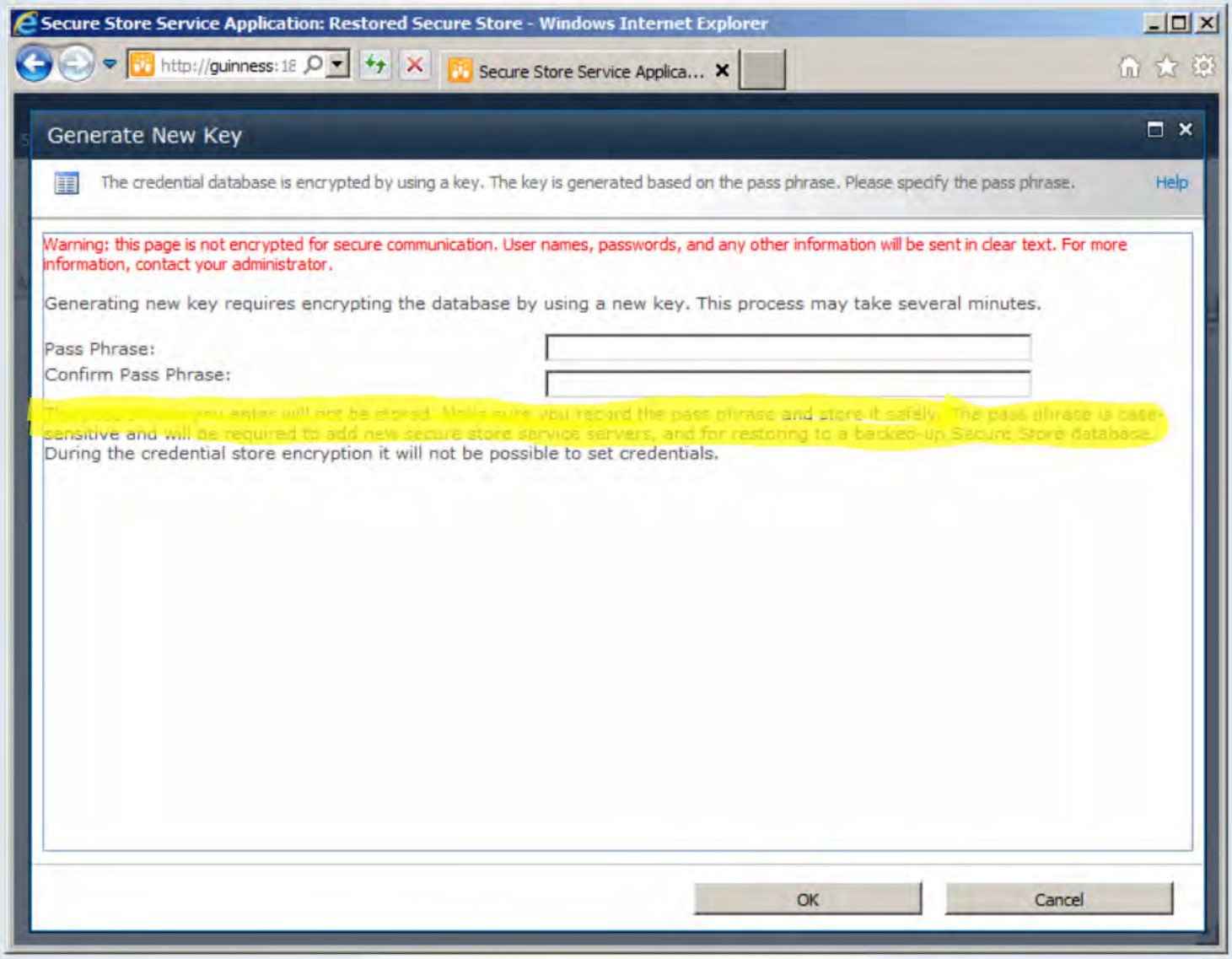
Managed Metadata



Secure_Store_Se

StateService_fd


Secure Store Service Application: Restored Secure Store - Windows Internet Explorer
http://guinness:18
Secure Store Service Applica...
Site Actions
Browse
Edit
SPDEMO\s0ladmin
New
Delete
Edit
Generate New Key
Refresh Key
Set
Set
Manage Target Applications
Key Management
Credentials
Permissions
Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards
Before creating a new Secure Store Target Application, you must first generate a new key for this Secure Store Service Application from the ribbon.



Documentation in some form will be required for any protection strategy selected.

Search

- Service application special case (2010)
- Part of an SSP instance (2007)

Where is it?

- SQL Server houses admin, crawl and property store databases (for 2010)
- File system houses index partition(s)

MOSS 2007 only has a single search database per SSP

Protection

- Synchronization between index partitions and crawl database is critical
- SharePoint backups or a solution that engages the SharePoint VSS writer

MOSS 2007 only has a single search database per SSP

Related targets

"important to remember"

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

Solution packages

- .wsp files that are added to the farm to deploy custom code, Features, etc.

Where are they?

- Ultimately depends on your processes

Worth protecting?

- Absolutely. Backup is critical in most cases

Protection

- For centrally managed solution packages, basic file protection/backup is common
- Configuration-only backup with SP2010

You are packaging your customizations this way ... right?

If you answered "no," then pay attention ...

"Centrally managed"

vs

"Decentralized" customizations

Centrally managed	Decentralized
Assets and resources packaged into a single .wsp (cab) file	Assets and resources are loose or packaged in another form (e.g., MSI)
SharePoint stores customization files in farm solution store (in farm config DB) and knows "what" goes "where"	SharePoint is unaware of the files that constitute the customization and does not track them in any way
SharePoint manages deployment and retraction of customization files where needed across farm	Administrator is entirely responsible for ensuring file and configuration changes happen (usually manually)
During a restore or new farm member addition, SharePoint works its magic to get assets and resources deployed	Restores and new farm member additions mean more manual administrator intervention

Tracking related backup targets is dramatically easier when centrally managed solutions are used.

SharePoint Root

- The guts of SharePoint's core file system
- Also known as the 12-hive (for 2007)

Where is it?

- C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14 (or \12)

Worth protecting?

- Depends on customization usage and deployment patterns
- "Yes" for decentralized customizations

Protection

- File system backup

IIS Configuration

- Settings used to serve web pages by IIS
- Covers app pools, ports, protocols, etc.

Where is it?

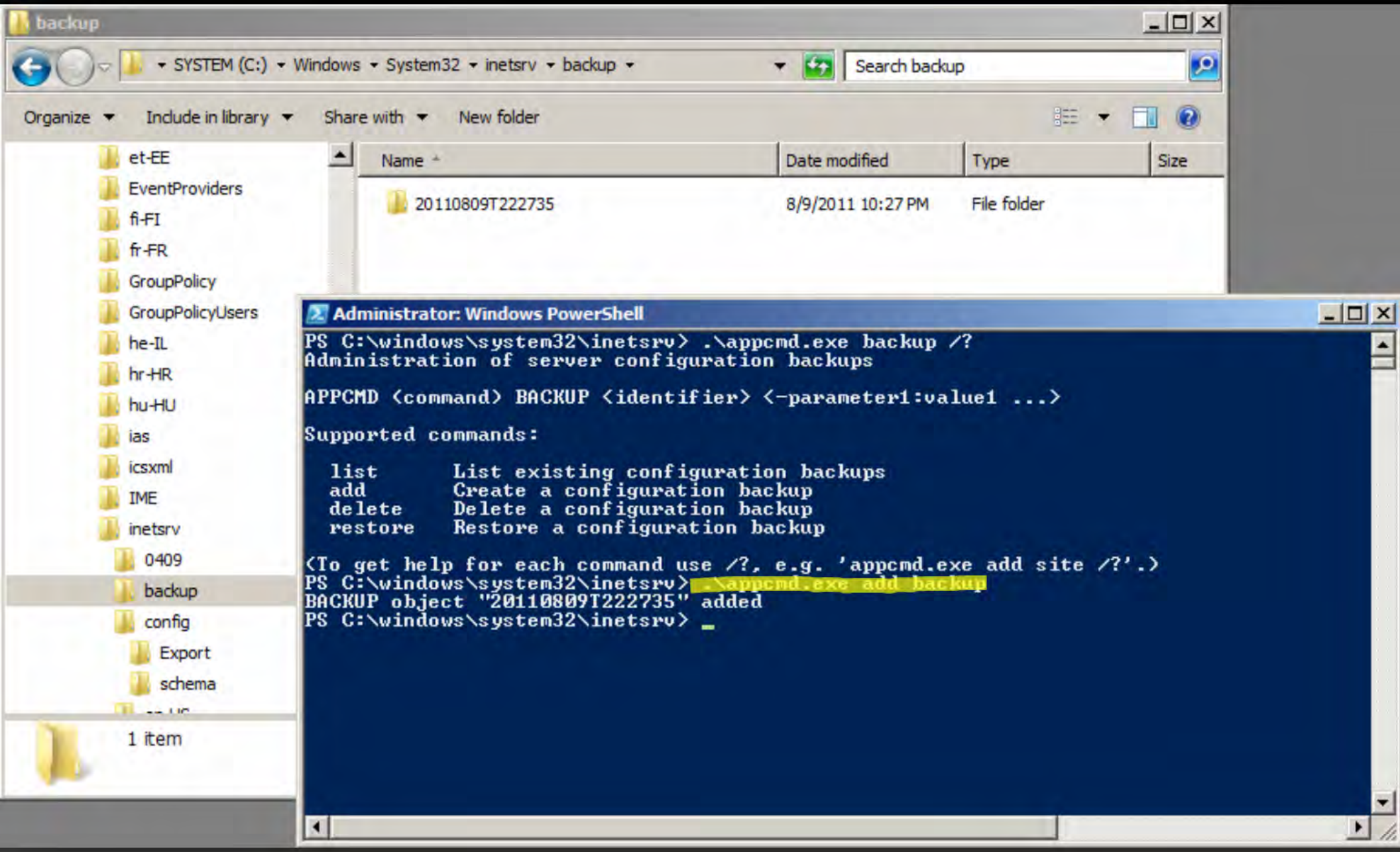
- C:\Windows\system32\inetsrv by default (IIS6 Metabase and IIS7.x config files)

Worth protecting?

- Some of it, but there is significant redundancy with information that SharePoint stores

Protection

- File copy*, appcmd.exe*, documentation


backup
SYSTEM (C:) ▸ Windows ▸ System32 ▸ inetsrv ▸ backup
Search backup
Organize
Include in library
Share with
New folder
et-EE
EventProviders
fi-FI
fr-FR
GroupPolicy
GroupPolicyUsers
he-IL
hr-HR
hu-HU
ias
icsxml
IME
inetsrv
0409
backup
config
Export
schema
1 item
Name
Date modified
Type
Size
20110809T222735
8/9/2011 10:27 PM
File folder
Administrator: Windows PowerShell
PS C:\windows\system32\inetsrv> .\appcmd.exe backup /?
Administration of server configuration backups
APPCMD <command> BACKUP <identifier> <-parameter1:value1 ...>
Supported commands:
list List existing configuration backups
add Create a configuration backup
delete Delete a configuration backup
restore Restore a configuration backup
<To get help for each command use /?, e.g. 'appcmd.exe add site /?'.>
PS C:\windows\system32\inetsrv> .\appcmd.exe add backup
BACKUP object "20110809T222735" added
PS C:\windows\system32\inetsrv> _

Certificates

- Commonly used to encrypt communications with sites (SSL)

Where are they

- Local machine certificate store
- Accessible via MMC or IIS Manager

Worth protecting?

- Yes

Protection

- Interactive export from MMC or IIS Manager
- Export via PowerShell or code

Pay attention to where SSL terminates to find certs

IIS web root

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

Where is it?

- C:\inetpub\wwwroot\wss\VirtualDirectories
- Other paths possible

Worth protecting?

- Usually for web.config files et al
- "Yes" for decentralized customizations

Protection

- File system backup, documentation

Global Assembly Cache

- Microsoft .NET Framework GAC is a repository for shared libraries (DLLs) and native images

Where is it?

- C:\Windows\assembly

Worth protecting?

- Sometimes (typically for decentralized customizations)

Protection

- File system backup*

Avoid complete overwrites when restoring

Registry

- Windows Operating System database for system and program information storage

Where is it?

- C:\Windows\System32\config (mostly)
- User profile area (for each user's HKEY_CURRENT_USER settings)

Worth protecting?

- Some branches (e.g., HKLM\SOFTWARE\Microsoft\Office Server\14.0\...)

Protection

- Regedit export, PowerShell, documentation

Bits and bytes

- The (often-forgotten) files and installers need to rebuild a SharePoint environment: setup files, OWAs, SPs, CUs, iFilter packs, SQL client install, etc.

Where are they?

- Typically scattered on shares or media

Worth protecting?

- If your DR strategy involves rebuilding the SharePoint farm, then yes

Protection

- External media/disks, replicated storage

Edge cases and esoteric targets

sometimes confused with the dark arts ...

- .NET framework config folders
- Remote BLOB storage (RBS)
- SQL Server TDE
- External data sources
- Single server farm ...

.NET Framework config

- System-wide configuration files and defaults for .NET applications

Where are they?

- C:\Windows\Microsoft.NET\Framework\v…\Config and \Framework64\v...\Config

Worth protecting?

- Yes if you've made alterations to the machine.config or similar files

Protection

- File system backup, documentation

Remoted BLOBs

- Alternate location where binary large objects (BLOBs) are stored when RBS is in-use within the farm.

Where are they?

- Varies and depends on RBS provider
- Some form of file storage isn't unusual

Worth protecting?

- Absolutely critical if you use RBS

Protection

- Check RBS provider guidance.
- For file share RBS storage, backup of RBS store commonly follows content DB backup

SQL Server TDE

- TDE = Transparent Data Encryption
- Real-time encryption/decryption of SQL Server data and log files

Where is it?

- SQL Server master DB or EKM module
- EKM = extensible key management

Worth protecting?

- Yes

Protection

- Backup of certificate (from master DB) or asymmetric key (from EKM) yields 2 files
- Save files for later recovery or DB transport

External data sources

- Data that is consumed (and presented) by SharePoint but resident elsewhere

Where is it

- Depends on environment. Examples include BCS sources and SQL Server Reporting Services databases

Worth protecting?

- Highly variable and driven by business factors and SLAs - not technology

Protection

- Varies by data source and platform

The single server farm

If you have an all-in-one farm and want to maximize usage of built-in platform tools:

- Use built-in Windows Server Backup (2008, 2008R2)
- Register the SharePoint VSS Writer
  - stsadm.exe -o registerwsswriter
- Perform your backups as desired
- Protects entire server, including consistent SP backups
- Bare metal restore capability
- Tough to beat for a free catastrophic protection solution

Wrap-up

Your targets are unique like 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.

References

"Document farm configuration settings (SharePoint Server 2010)"
- http://tinyurl.com/SPDRFarmDoc2010

"Overview of SharePoint Foundation and the Volume Shadow Copy Service"
- http://msdn.microsoft.com/en-us/library/cc264314.aspx

"Backup and restore customizations (Windows SharePoint Services)"
- http://technet.microsoft.com/en-us/library/ee216349(office.12).aspx

"Configuration-Only Backup and Restore in SharePoint 2010"
- http://SharePointInterface.com/2010/09/10/configuration-only-backup-and-restore-in-sharepoint-2010/

"Overview of Remote BLOB Storage (SharePoint Foundation 2010)"
- http://technet.microsoft.com/en-us/library/ee748607.aspx

"Understanding Transparent Data Encryption (TDE)"
- http://msdn.microsoft.com/en-us/library/bb934049.aspx

"Plan for backup and recovery (SharePoint Server 2010)"
- http://technet.microsoft.com/en-us/library/cc261687.aspx

"Scheduling SQL backups for SharePoint"
- http://www.toddklindt.com/blog/Lists/Posts/Post.aspx?ID=248

Please complete and turn in your Session Evaluation Form as your entry for Prizes at the end of event prize raffle.

Presenter:

Sean P. McDonough

Session Name:

Selecting and Protecting the Right SharePoint Backup Targets

- Remember to visit the exhibit hall.

- Get to know your user groups to find out about local activities and events in your area.

- Make sure you stick around for the closing session and turn in your evaluation forms to be eligible for the prize raffles.

SharePoint Cincy

MARCH 16, 2012

cai
CENTER FOR APPLIED INFORMATICS
NORTHERN KENTUCKY UNIVERSITY™

Microsoft®

MAX
max technical training

K2®

SOGETI

ascendum
Rise Together

Aspect

newsgator

PCMS
IT Advisor Group

CBTS
TECHNOLOGY SOLUTION ARCHITECTS

BRAINSTORM
Teaching Software. Teaching People.

KnowledgeLake
The SharePoint® ECM Company

#SPcincy2012 on Twitter
www.sharepointcincy.com

Finding me

Sean P. McDonough

Blog: http://SharePointInterface.com
Email: sean@SharePointInterface.com
LinkedIn: http://www.linkedin.com/in/smcdonough
Twitter: @spmcdonough

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

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