# Disaster recovery

http://www.cs.vsb.cz/navrat

*Jan Žák*

Správa počítačových systémů
(SPS)

Microsoft CERTIFIED Systems Engineer
Microsoft CERTIFIED Trainer

## What Is Disaster Recovery?

- Resuming operations after a disaster
- Implementing a disaster recovery plan:
  - Replacing damaged components
  - Restoring data
  - Testing before resuming

Správa počítačových systémů
(SPS)

## Disaster-Recovery Preparation Guidelines

- Develop a backup strategy
- Test your backup strategy and assess its product
- Include an alternate backup that is stored offsite
- Backup System State data
- Install the Recovery Console as a startup option
- Store the installation CD for accessibility in a crisis

Správa počítačových systémů
(SPS)

## Lesson: Backing Up Data

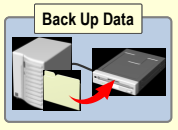
- Overview of Backing Up Data
- Who Can Back Up Data?
- What Is System State Data?
- What Is the Backup Utility?
- Types of Backup
- What Is ntbackup?
- What Is Automated System Recovery?
- Practice: Backing Up Data

Správa počítačových systémů
(SPS)

## Overview of Backing Up Data

Backups:

- Copy data to alternate media
- Prevent data loss
- Require the following considerations:
  - –Which files need back up?
  - –What is the backup frequency?
  - –What is the need for network backup?






## Who Can Back Up Data?

- File owners and users with read permissions
- Users with rights to the backup files and directories
- Groups on local servers:
  - Administrators
  - Backup operators
  - Server operators



## What Is System State Data?

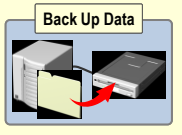
System-specific data that must be backed up as a unit

| Component | Included in System State |
|---|---|
| Registry | Always |
| Boot files, including system files | Always |
| Certificate Services database | If it is a Certificate Services server |
| Active Directory directory service | If it is a domain controller |
| SYSVOL Directory | If it is a domain controller |
| Cluster service information | If it is within a cluster |
| IIS metadirectory | If it is installed |
| System files that are under Windows File Protection | Always |



## What Is the Backup Utility?

- Use Backup Utility to:
  - –Back up files and folders
  - –Back up System State data
  - –Schedule a backup
  - –Restore data
- Back up open files with Volume Shadow Copy
- Back up to various media types





## Types of Backup

- Some backup types use the archive attribute
- Some backup types work together

| Type | Files backed up | Clears archive attribute |
|---|---|---|
| **Normal or Full** | Selected files and folders | Yes |
| **Copy** | Selected files and folders | No |
| **Differential** | Selected files and folders that were modified after the last normal backup | No |
| **Incremental** | Selected files and folders that changed after the last normal or incremental backup | Yes |
| **Daily** | Selected files and folders that changed during the day | No |



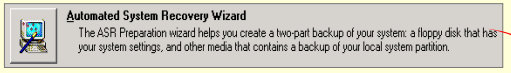
## What Is ntbackup?

- **Use the ntbackup command-line tool to:**
  - Back up System State data
  - Back up files
  - Back up using batch files
- **Understand the ntbackup limitations**
  - Backs up whole folders, not selected files
  - Does not accommodate wildcard characters



## What Is Automated System Recovery?

- A recovery option in the Backup utility
- Operating system backup
- Does not include data files
- Creates a floppy disk with configuration information




To back up all data, choose the All information option



## What Is a Scheduled Backup Job?

## What Are Scheduled Backup Options?

| Schedule options | Executes the job: |
|---|---|
| **Once** | At a specific time on a specified date |
| **Daily** | At a specified time each day |
| **Weekly** | At a specified time on specified weekdays |
| **Monthly** | At a specified time on a specified day each month |
| **At startup** | The next time the system is started |
| **At logon** | The next time the job owner logs on |
| **When idle** | After the system is idle for a specified period |



## Best Practices for Backup

- Develop a backup strategy and test it
- Train appropriate personnel
- Backup volume and System State data simultaneously
- Create an Automated System Recovery Backup set
- Make copies
- Perform trial restorations
- Secure media
- Use the default Volume Shadow Copy backup



## What Is Restoring Data?


Restoring data rewrites:

- Files and folders
- System State data

The ASR Restore:

- Reads recovery data for disk configuration
- Restores book disk signatures, volumes, and partitions
- Installs a recovery version of Windows
- Initiates the restore from backup



## Guidelines for Restoring Data

- Plan and test restoration strategies
- Set permissions for systems administrators
- Verify connections to each restore location
- Ensure access to network based media
- Consider data recovery for EFS files restored at alternate locations

## What Are Shadow Copies?

- Shadow copies provide iterative versions of network folders
- Use shadow copies to:
  - Recover files
  - Review previous versions
- Shadow copies are:
  - Enabled per volume
  - Not a replacement for regular backups
  - Allocated storage limits versions



## Previous Versions Client Software for Shadow Copies

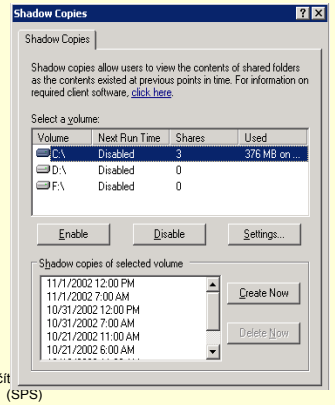
- Previous Versions client software is stored on the server

  %systemroot%\system32\clients\twclient\x86 directory
- Use to access previous versions of files



## Shadow Copy Scheduling

- Default schedule is 7:00 A.M. and noon
- Create a shadow copy schedule based on:
  - –Volume of changes
  - –Importance of changes
  - –Storage limitations
- Test a schedule with a small group






## What Is Restoring Shadow Copies?

A server saved copy of a file or folder is restored to the client

| Characteristics of Shadow Copies | |
|---|---|
| **If…** | **Then** |
| **No previous versions** | **The file was not modified after the last save** |
| **Restoring a folder** | **The current version is deleted** |
| **Restoring a file** | **File permissions are not changed** |
| **Properties does not include a Previous Versions tab** | **Shadow copies might not be enabled** |
| **Copying a file** | **File permissions are set to default** |

## Best Practices for Using Shadow Copies

- Consider the work patterns of users
- Be aware of the limitations of mounted drives
- Do not enable shadow copies on dual-boot computers
- Store shadow copies in a separate volume and on separate disk
- Shadow copies do not replace backups
- Do not schedule more than one copy in an hour
- Before deleting a volume that is being shadow copied, delete the scheduled task for creating shadow copies



## What Is Safe Mode?

A Windows Server 2003 tool for system problem-solving

**Uses these default settings:**

- VGA mode
- Mouse driver
- No network connections
- Minimum device drivers required to start Windows

**Use safe mode to:**

- Diagnose problems
- Change server settings
- Recover from viruses



## What Are Safe Mode Options?

| Option | Description | Use |
|---|---|---|
| **Safe Mode** | Loads only basic files and drivers | When Windows is not starting in Normal mode |
| **Safe Mode with Networking** | Loads only basic files and drivers, plus network connections | To access troubleshooting tools that are on the network |
| **Safe Mode with Command Prompt** | Loads only basic files, drivers, and a command prompt interface | When Safe Mode will not start properly |



## What Is Last Known Good Configuration?

- Restores registry information and drivers
- Resolves startup problems after a change
- Does not solve problems caused by corrupted or missing drivers or files
- Logging on updates the Last Known Good Configuration

## What Is the Recovery Console?

**Includes:**

- A minimal version of Windows Server 2003
- A command-line interface

**Allows administrators to:**

- Enable or disable device drivers or services
- Copy files from the installation CD for the operating system, or copy files from other removable media
- Create a new boot sector or new master boot record (MBR)



## Recovery console: install/start

- <cd>\I386\winnt32.exe /cmdcons
- <cd>\bootdisk\makebt32.exe (makeboot.exe)
- Start PC from CD, select „R – repair“ option



## Recovery Console options

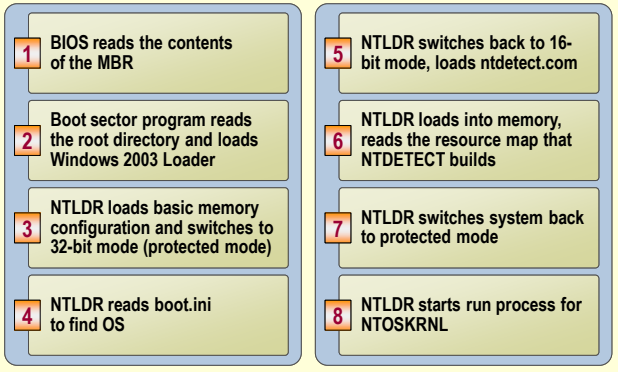
- attrib del fixboot more set batch delete fixmbr mkdir systemroot bootcfg dir format more type cd disable help net chdir diskpart listsvc rd chkdsk enable logon ren cls exit map rename copy expand md rm dir
- http://support.microsoft.com/kb/314058



## What Is a Windows Startup Disk?

- Allows Windows startup on a computer with a faulty boot sequence
  - Damaged boot sector
  - Damaged master boot record (MBR)
  - Missing or damaged Ntldr or Ntdetect.com files
  - Incorrect Ntbootdd.sys driver
- Includes:
  - Ntldr
  - Ntdetect.com
  - Boot.ini
  - Ntbootdd.sys

## How Startup Files Function






## Selecting Disaster-Recovery Methods

| Tool | Use When |
|---|---|
| **Safe Mode** | A problem prevents the normal Windows Server 2003 startup |
| **Last Known Good Configuration** | The configuration is incorrect |
| **Backup** | You need to create a duplicate copy of data on your hard drive and then archive the data on another storage device |
| **Recovery Console** | You cannot fix the problems by using one of the startup methods |
| **Automated System Recovery (ASR)** | Other repair operations fail |



## Recovery options for DC‘s

**(AD database is corrupted)**

- **Rebuild**
  - OS reinstall, promote server to DC, replicate
  - ☺ Known recovery time and results
- **Restore**
  - Using NTBACKUP to restore usable system state, replicate
- **Repair**
  - Using NTDSUTIL (ESENTUTL) to database repair, check DB integrity
  - ☹ Use as last chance



## How to reset DSRM password

1. ntdsutil
2. set dsrm password
3. reset password on server null

or

reset password on server <*server_name*>

*NOTE: Use „NET USER ADMINISTRATOR *“ for Windows 2000 DC in DSRM mode or user „Setpwd“* (SP2 only)

## How objects are deleted from AD

- When an object is deleted, it is not removed from the Active Directory database.
- Instead, the object is marked for deletion at a later date.
- This mark is then replicated to other domain controllers. Therefore, the garbage collection process starts by removing the remains of previously deleted objects from the database.
- These objects are known as *tombstones*.
- Next, the garbage collection process deletes unnecessary log files.
- Finally, the process starts a defragmentation thread to claim additional free space.



## After object deletion

- When an object is transformed into a tombstone ALL almost attributes values, except those mandatory and additionally manually configured, are stripped from the deleted object.
- The values of the following attributes are preserved during a deletion:
  - objectGUID, objectSid, nTSecurityDescriptor and uSNChanged
  - Additionally on W2K3 SP1 DCs: sIDHistory



## Backup Limitations

- Backup life = tombstonelifetime value
  - Default = 60 days old (or 180 days)
  - Password change interval = 30 days
  - Password history = 2 (current and previous)
  - Backup useful life = 60 days or two default password changes
  - Old backups can reintroduce tombstoned objects
- Schema rollback is not supported!!!!!



## Nonauthoritative Restore

- What is it?
  - Restore to known good point using Ntbackup
  - Reboot into Active Directory mode to sync changes
- When to use
  - Recover from hardware failure
  - Return to known good state on single domain controller
- Options
  - Rebuild server from scratch. Re-run Dcpromo.
  - Restore machine to a known good point and sync deltas.

## Authoritative Restore

- What is it?
  - Restore to known good point using Ntbackup
  - Make objects on reference domain controller as “master copy” for Active Directory
- When to use
  - Accidental deletion or modification of objects or containers in the Active Directory
  - Corruption of objects/attributes in the directory
- Options
  - Find a good domain controller that has the objects and make it authoritative
  - Restore from a backup that contains the objects and make it authoritative



## Authoritative Restore (cont.)

- Boot into offline restore mode
  - Press F8 during boot phase
  - Log on with offline administrator account
- Mark objects in Ntdsutil as authoritative
  - Find machine with objects or restore them
  - Restore subtree or entire database (rare)
- Best practice
  - Use most specific distinguished name path needed for recovery
  - Restore Active Directory over Terminal Services– Q256588



## How to undelete objects in AD

- Authoritative restore (almost all attributes are preserved on W2k3 SP1 ☺, DC is offline during restore, backup may be corrupted ☹ )
- LDF (from previously exported file – but with new SID and GUID !!! ☹ )
- LDP (change „isDeleted“, „distinguishedName“, most attributes are gone ☹)
- ADRESTORE (same as with LDP, morec comfortable)
- Lag DC (DC in other site, configured to obtain updates in 3 days for ex.)
- 3 rd parties tools also exist ($$$ ☹ )



## AD DB is corrupted -first/last chance – recover/repair database

- In DSRM, run NTDSUTIL
- files
- recover (or repair)

OR

- esentutl /f <path>\ntds.dit (or esentutl /p)
- delete all .log files (or backup them)

- Import missing objects from .ldf file

## Integrity check

- By using the **integrity** command, you can detect low level (binary level) database corruption. The **integrity** command reads every byte of the data file. Therefore, depending upon the size of your database, the process might take a considerable amount of time.
- The **integrity** command also makes sure that the correct headers exist in the database itself and that all of the tables are functioning and are consistent. This is used while in Directory Services Restore mode. If errors are encountered, they are recorded on the log files.



## Semantic check

- **Reference count check.** Counts all of the references from the data table and the link table to ensure they match the listed counts for the record. (For more information about data and link tables, see the section on Active Directory Data Storage in the Distributed Systems Guide of the Windows 2000 Resource Kit.) This also ensures that each object has a GUID, distinguished name and nonzero reference count. For a deleted object, the check ensures that the object has a deleted time and date, but does not have a GUID or a distinguished name.
- **Deleted object check.** Ensures the object has a deleted time and date, and a special relative distinguished name.
- **Ancestor check.** Checks to determine if the current distinguished name tag (DNT) is equal to the ancestor list of the parent and the current DNT.
- **Security descriptor check.** Checks for a valid descriptor, ensuring that it has a control field, and that the discretionary access control list is not empty. If there are deleted objects without a discretionary control access list, a warning is printed.
- **Replication check.** Checks the UpToDate vector in the directory partition head to ensure that the correct number of cursors exists. It also checks to see that every object has property metadata vector. For the instance type of the object, it checks the metadata, the up-to-dateness vectors, the sub references, and partial attribute.



## Check/fix ntds.dit

- In DSRM, run NTDSUTIL
- files
- integrity
- If OK, try tro reboot DC

- semantic database analysis
- go

- semantic database analysis
- go fixup

- try offline defragmentation

- If there are more DC‘s, demote your DC and promote it again
- If you have no more DC‘s, try to restere server from backup
- Rebuild your domain… OR…



## How to cleanup AD from „Ghosts“

- Removing DC
- Removing DC after unsucessfull removing
- Remove domain when no more DC‘s available

## DCPROMO should be used, but if cannot be…

- Information about config:

  CN=NTDS Settings,CN=<servername>,CN=Servers,CN=<sitename>,CN=Sites,CN=Configuration,DC=<domain>...

- The attributes of the NTDS Settings object include data representing how the domain controller is identified in respect to its replication partners, the naming contexts that are maintained on the machine, whether the domain controller is a global catalog server, and the default query policy.
- The NTDS Settings object is also a container that may have child objects that represent the domain controller's direct replication partners. This data is required for the domain controller to operate in the environment, but is retired upon demotion.
- http://support.microsoft.com/kb/216498

AD Distaster Recovery