Data storing and data security

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

Jan Žák

Agenda

- File systems
- Benefits of using NTFS
- Basic and dynamic disks
- Faul tolerance volumes
- EFS
- IPSec
- Backup

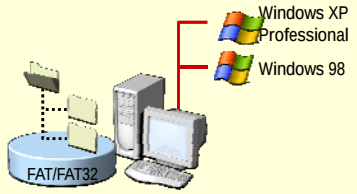
Some of MS filesystems...

	FAT12 (1977/MS DiscBASIC)	FAT16 (1988/MS-DOS)	FAT32 (1996/W95)	NTFS (1993/NT)
Max filesize	32 MiB	2 GiB	4 GiB	16 TiB (16 EiB teor.)
Max # of files	4 077	65 517	268 435 437	4 294 967 295
Max volumesize	32 MiB	2 GiB (or 4 GiB)	8 TiB	256 TiB (16 EiB teor.)
Security (ACL)	No	No	No	Yes

Using FAT or FAT32

FAT or FAT32:

- Works well on small disks with simple folder structures
- Supports dual-boot configurations



Using NTFS

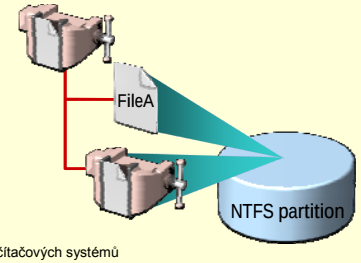
NTFS Provides:

- Improved reliability by identifying and not using bad sectors
- Enhanced security by using EFS and file permissions
- Improved management of storage growth
- Support for large volume sizes

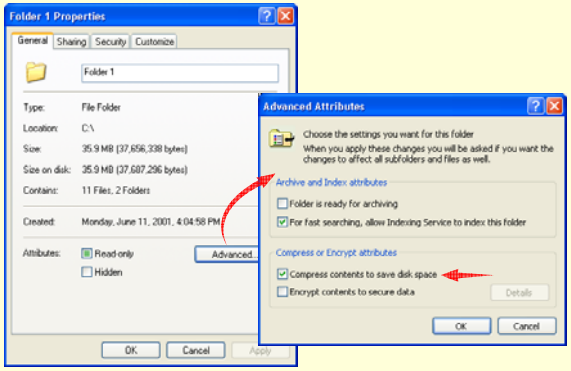
You can convert FAT to NTFS with CONVERT command.

Defining Compressed Files and Folders

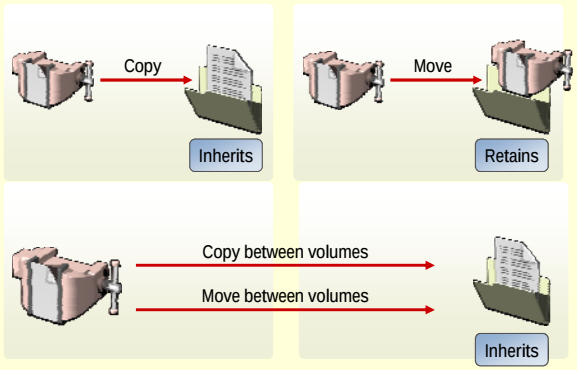
- NTFS files and folders have a compression state
- When accessed, files are automatically uncompressed
- Space allocation is based on uncompressed file size
- Compressed files and folders can be designated by color



Compressing Files and Folders



Copying and Moving Compressed Files and Folders



Introduction to EFS

EFS:

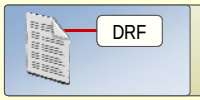
- Is transparent to users and applications
- Is accessible only to authorized users
- Enables specification of a data recovery agent
- Encrypts files locally or across the network
- Enables encrypted files and folders to be designated by color

Encrypting a Folder or File

Encrypt contents to secure data

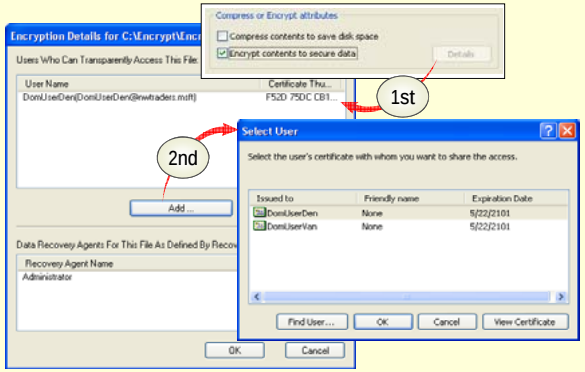
When file is saved, it is encrypted by using file encryption keys

The user's file encryption key is stored in the Data Decryption Field



If designated, the recovery agent's file encryption key is stored in the Data Recovery Field in the file header

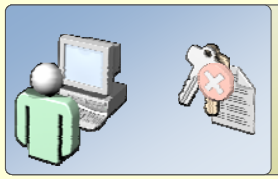
Adding Authorized Users



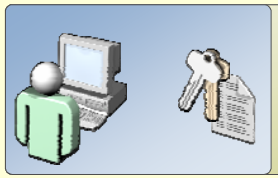
What Is an EFS Recovery Agent?

- Authorized to decrypt data
- Required when users are deleted
- Required when local user passwords are reset
- The recovery key can be exported

Recovering an Encrypted Folder or File



Owner's key is unavailable



Recovery agent uses his private key to recover the file

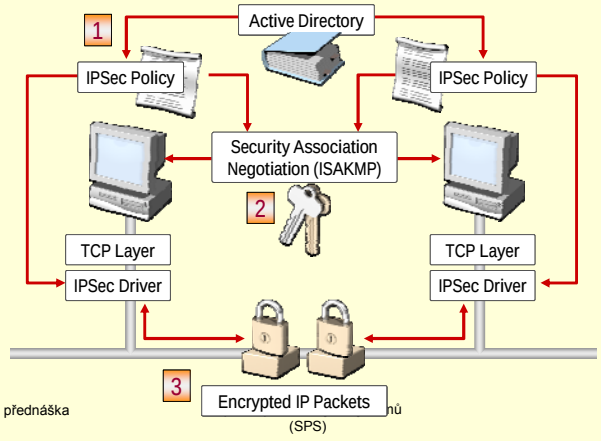
What Is IPSec?

IPSec verifies, authenticates, and encrypts IP packets to provide secure network transmissions

IPSec provides:

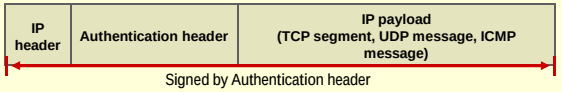
- Mutual authentication before and during communications
- Confidentiality through encryption of IP traffic
- Integrity of IP traffic by rejecting modified traffic
- Protection from replay attacks

How IPSec Works

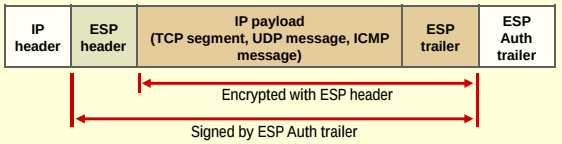


IPSec Protocols

AH provides authentication, integrity, and anti-replay protection

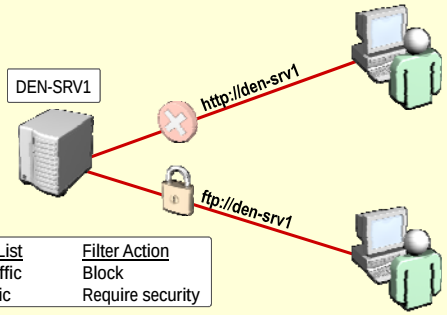


ESP provides confidentiality, authentication, integrity, and anti-replay protection



IPSec Packet Filtering

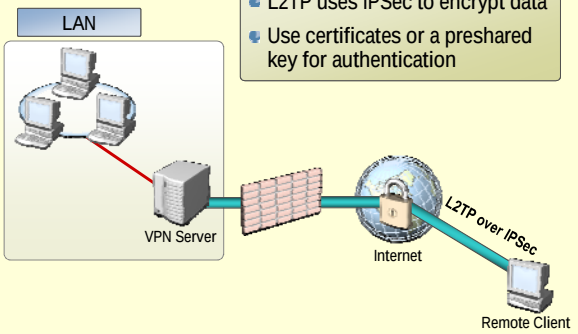
Packet-filtering rules allow a computer to determine what traffic is allowed and the level of security required



IP Filter List	Filter Action
HTTP traffic	Block
FTP traffic	Require security

IPSec Configurations for Virtual Private Networking

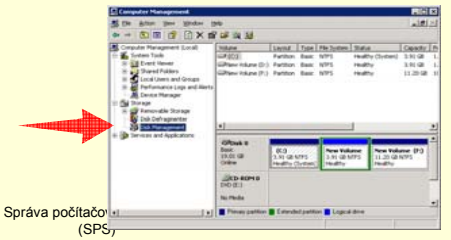
- L2TP uses IPSec to encrypt data
- Use certificates or a preshared key for authentication



Managing Disks

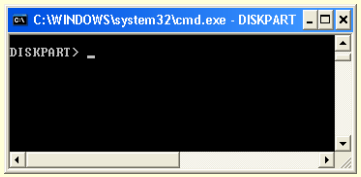
What Is Disk Management?

- A snap-in located in the Computer Management console
- Use to view disk information and perform disk management tasks
- Enables you to perform most disk-related tasks without shutting down the system or interrupting users



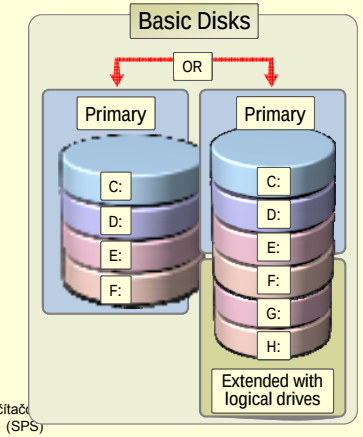
What Is the DiskPart Tool?

- With the DiskPart command-line tool:
  - –Select an object, then type a command
  - –Use it to manage disks, partitions, and volumes
  - –Use scripts for repetitive tasks



What Is a Partition?

- A physical disk is sectioned into separate partitions
- Basic disks can have up to:
  - –Four primary partitions
  - –Three primary partitions and one extended partition
- Extended partitions are subdivided into logical drives



Basic Disks vs. Dynamic Disks

Benefits of basic disks include:

- Setup and Recovery Console access
- Disk utility availability

Benefits of dynamic disks include:

- Spanning multiple disks
- Volume limits per disk
- Fault-tolerant capability

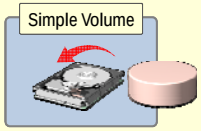
Results of Dynamic Disk Conversion

- Basic disk partitions become volumes
- Data on the disk is preserved
- The disk gains a disk group identity

Reverting a dynamic disk to a basic disk results in the loss of all partitions and data on the disk

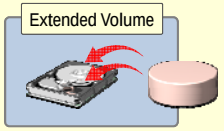
What Is a Simple Volume?

- Contains space on a single disk
- Can be created only on dynamic disks
- Can use the NTFS, FAT, or FAT32 file systems
- Can be extended if formatted with NTFS

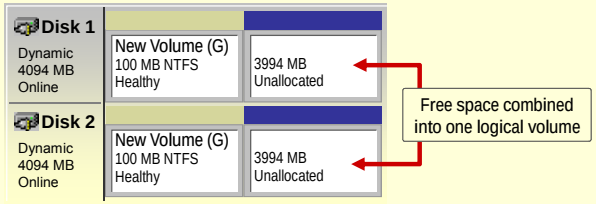


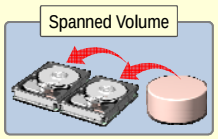
What Is an Extended Volume?

- Created by extending a simple volume onto unallocated space on the same disk or a different disk
- The unallocated space must be unformatted or formatted with a version of NTFS

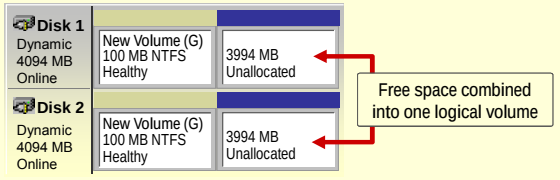


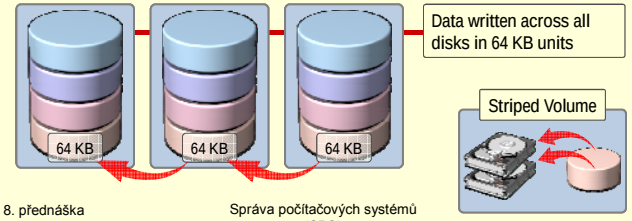
What Is a Spanned Volume?





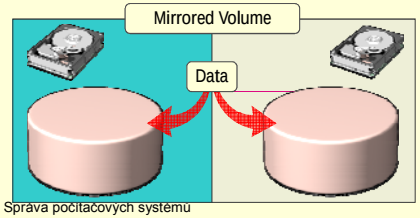
What Is a Striped Volume?



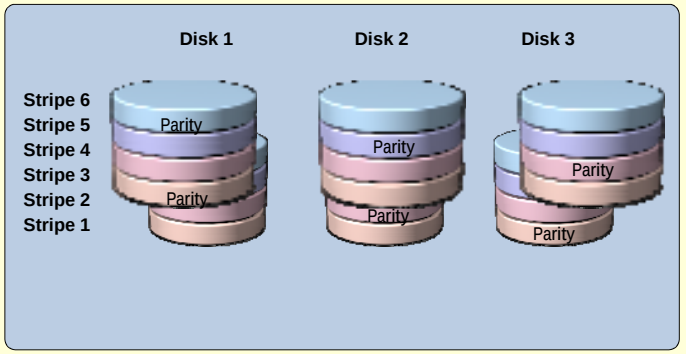


What Is a Mirrored Volume?

- Simultaneously written data to two volumes on two physical disks
- Almost any volume can be mirrored, including the system and boot volumes
- Many mirrored volume configurations use duplexing



What Is a RAID-5 Volume?

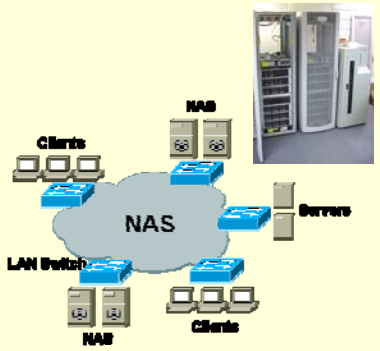


Software RAID vs. Hardware RAID

RAID Type	Benefits
Software RAID	• **Configured in Disk Management** • **Requires dynamic disks** • **Used mostly in smaller organizations** • **Failed mirrors may require boot.ini changes** • **Can move disks to any computer running Windows 2003 Server**
Hardware RAID	• **Configured with vendor utilities** • **Does not require dynamic disks** • **Higher performance** • **Does not require boot.ini changes** • **Can expand existing RAID-5 volumes**

What Is External Storage?

- External and auxiliary disk space
- External Array
- Storage Area Network (SAN)
- Network Attached Storage (NAS)



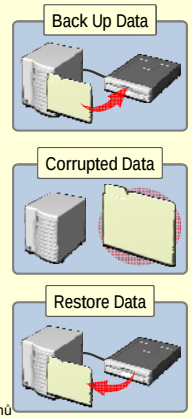
Backup

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 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



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 System State Data?

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

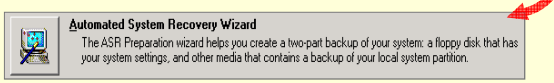
Component	Included in System State
Registry	Always
Boot files, including system files	Always
Certificate Services database	If it is a Certificate Services server
Active Directory directory service	If it is a domain controller
SYSVOL Directory	If it is a domain controller
Cluster service information	If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

Types of Backup

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 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

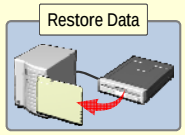


To back up all data, choose the All information option

What Is Restoring Data?

Restoring data rewrites:

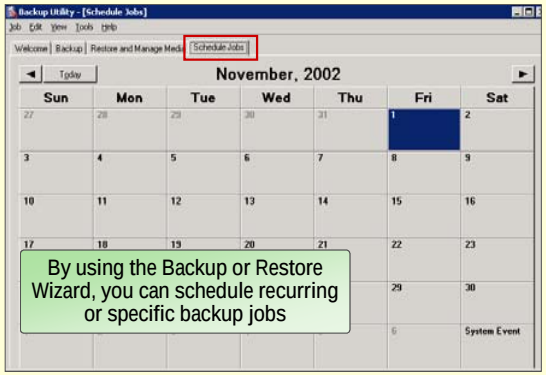
- Files and folders
- System State data



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

What Is a Scheduled Backup Job?



Guidelines for Restoring Data

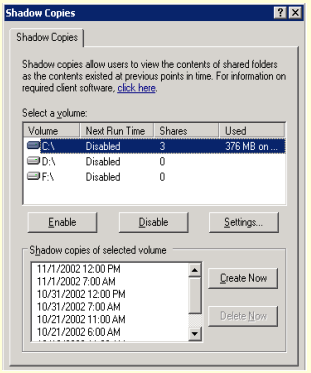
- Plan and test restoration strategies
- Set permissions for systems administrators
- Verify connections to each restore location
- Ensure access to network based media
- Consider data recovery for EFS files restored at alternate locations

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

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



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

Many more things you should consider...

- Antivirus programs
- Firewalls, disabling unnecessary services
- Decide to use/not use VPN and Wireless networks
- Data audit on NTFS/Alerting of incidents
- Permissions for users/groups
- Additional SW for encryptions (USB disks, laptops...)
- Procedures for users – what thay can and what they can not
- Password policy (max pass age, complex...)
- OS patching
- Physical security/access to servers
- Regular Risk Assessment, Predictive Analysis
- Human and Social elements (see Social Engineering etc)
- Disposing of admin/operators rights (can backup but can´t restore)
- Studying harder... ☺