

CNT 4603: System Administration Fall 2013

Managing Folder and File Security In AD

Instructor : Dr. Mark Llewellyn
 markl@cs.ucf.edu
 HEC 236, 4078-823-2790
 <http://www.cs.ucf.edu/courses/cnt4603/fall2013>

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida



Managing Folder And File Security In AD

- Resource sharing is a fundamental concept for a Windows Server 2008 network.
- Resource sharing is intended to increase the productivity of its users.
- The most frequently used resources on a server are folders (directories) and files, which might include written documents, spreadsheets, data files, databases, and multimedia files, etc..
- Some of these resources need to be kept secure because they contains sensitive information. Other resources are to be shared with limited groups to far-reaching audiences.
- Windows Server 2008 can securely protect folders and files or open them up to wide-scale sharing, depending on the need.



Managing Folder And File Security In AD

- Creating accounts and groups are the initial steps necessary to enable sharing resources. You will get some exposure to creating user accounts in a future project.
- The next step is to create Access Control Lists (ACLs) to secure these objects (folders and files) and to set them up for sharing.
- Windows Server 2008 has two types of ACLs: **discretionary** and **system control**.



Managing Folder And File Security In AD

- A **discretionary ACL (DACL)** is an ACL that is configured by a server administrator or owner of an object.
- For example, the server (system) administrator can configure who can access a company-wide shared folder containing personnel policies. Additionally, the human resources director may have their own folder of confidential information on the server that they might make available only to members of the Human Resources department. Because the HR director owns the folder, they can configure the folder's ACL to permit access to only members of their department.



Managing Folder And File Security In AD

- A **system control ACL (SACL)** contains information used to audit the access to an object.
- For example, a soft drink company decides to audit files that contain the secret recipes for their drinks. By configuring an SACL for each file that contains a recipe, the company monitors who has successfully viewed the file's contents and who has tried to view the contents, but failed because of DACL restrictions.
- When an SACL is not configured, this means that an object is not audited.
- The server administrator and object owners can configure DACLs and SACLs.



Managing Folder And File Security In AD

- Good security practices mean using DACLs and SACLs to protect the resources on your Windows Server 2008 network.
- The ACL-based object security techniques include the following DACL and SACL controls for folders and files:
 - Attributes
 - Permissions
 - Auditing
 - Ownership



Configuring Folder and File Attributes

- Windows Server 2008 continues to use attributes as defined in the NT file system (NTFS) and its predecessor File Allocation Table (FAT) file systems.
- Two basic attributes remain in the NTFS that are still compatible with FAT in older Windows operating systems: **read-only** and **hidden**.
- Both of these attributes are accessed from the General tab when you right-click a folder or file and click Properties, such as from Windows Explorer.



Configuring Folder and File Attributes

- When you check read-only for a folder, the folder is read-only, but not the files in the folder. This means the folder cannot be deleted from the command prompt (even though the folder attribute says “Only applies to files in a folder.” (See page 10.)
- When a file is checked as read-only, it also cannot be deleted from the command prompt.
- Most Windows Server 2008 server administrators ignore the read-only attribute box and set the equivalent protection in permissions instead, because the read-only permissions apply to the folder and can be inherited by its files.

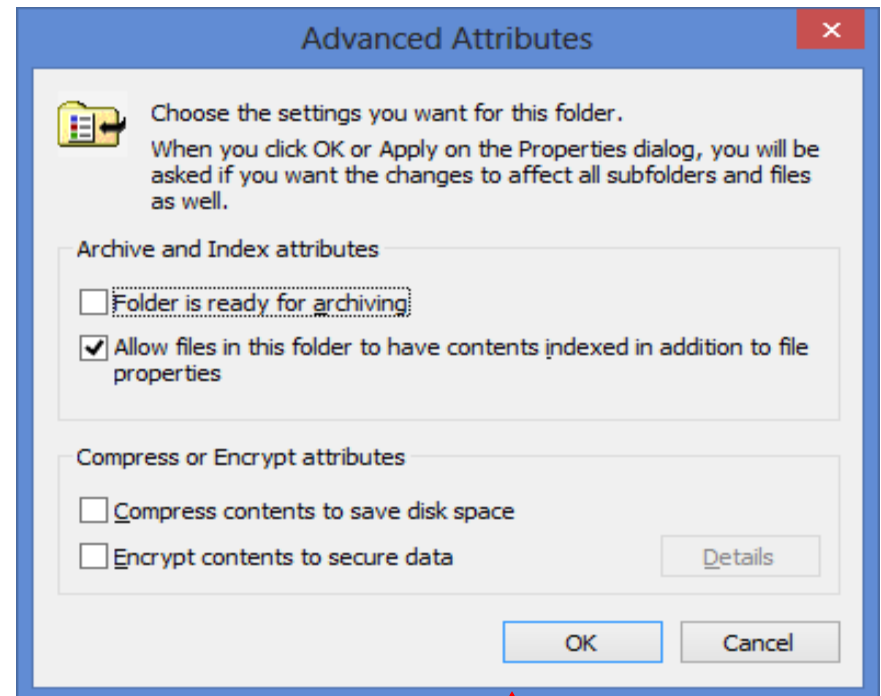
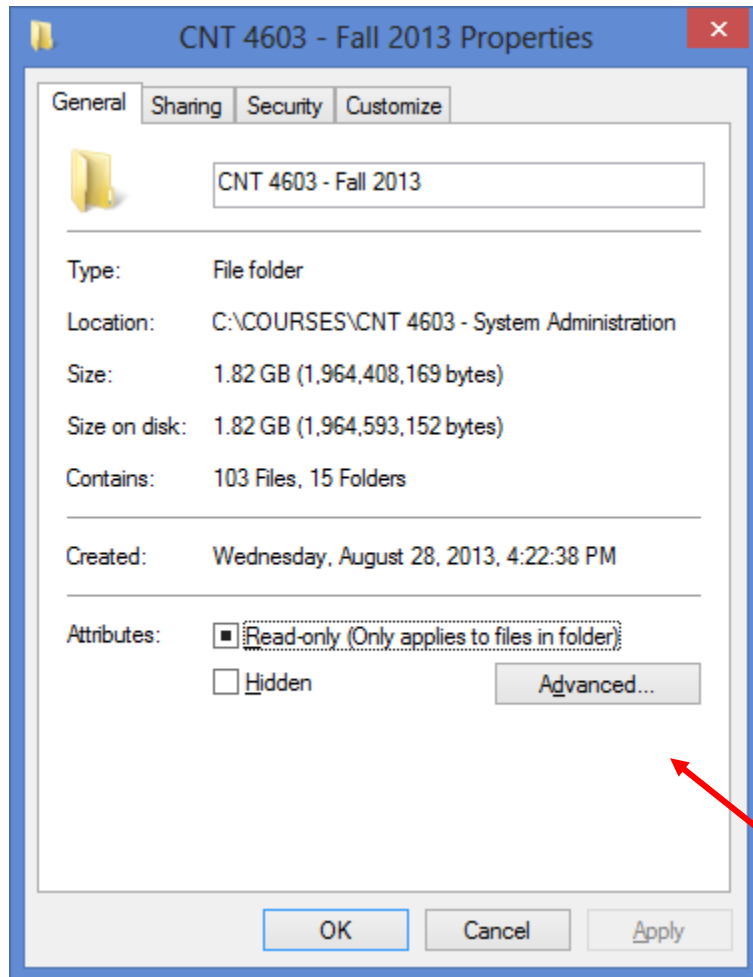


Configuring Folder and File Attributes

- Folders and files can be marked as hidden to prevent users from viewing their contents, which is a carryover from MS-DOS operating systems.
- The hidden attribute can be defeated by any Windows 98 and above client using Control Panel Folder Options to view hidden files and folders.
- The read-only and hidden attributes are on the General tab in an NTFS folder's or file's properties dialog box. In addition to these attributes, NTFS offers advanced or extended attributes, which are accessed by clicking the General tab's Advanced button (see page 10).



Configuring Folder and File Attributes



Click the Advanced button to bring up this dialog box



Configuring Folder and File Attributes

- The advanced attributes are archive, index, compress, and encrypt.
- When you make a change to an attribute in the Advanced Attributes dialog box in a folder's properties, you'll see a message box with the option to apply that change to only the folder and the files in that folder or to apply the change to the folder, its files, and all subfolders and files within the folder.



The Archive Attribute

- The archive attribute (Folder is ready for archiving – see page 10) – is checked to indicate that the folder or file needs to be backed up because it is new or changed.
- Most network administrators ignore the folder archive attribute, but instead rely on it for files. Files, but not folders, are automatically flagged to archive when they are changed.
- File server backup systems can be set to detect files with the archive attribute to ensure those file are backed up. The backup system ensures each file is saved following the same folder or subfolder scheme as on the server.



Index Attribute vs. Windows Search Service

- The index attribute and accompanying Indexing Service are legacy features for continuity with earlier operating systems, such as Windows Server 2000 and 2003.
- The NTFS index attribute (Index this folder for faster searching – see page 10) is used to index the folder and file contents so that the file name, text, creation or modification date, author, and other properties can be quickly searched in Windows Server 2008.
- The index attribute marks a folder's contents or a specific file to be indexed through the Indexing Service. The Indexing Service creates a catalog of documents to be tracked and searched.



Index Attribute vs. Windows Search Service

- Windows Server 2008 offers a newer, faster search service called Windows Search Service.
- This service is meant to replace using the index attribute and the Indexing Service, and it is recommended that you use this replacement – you can't use both the Windows Search Service and the Indexing Service at the same time.
- When you try Windows Search Service, you'll probably be surprised by its speed compared with the old Indexing Service.
- To use Windows Search Service, you must install the File Services role via the Server Manager. You'll do this in a later project.



Index Attribute vs. Windows Search Service

- Some files that are not conducive to searches, such as system files, are not included. These files are excluded to help reduce the size of the index catalog as a way to keep searches as fast as possible.
- Whenever you open a window, such as Windows Explorer, that has a Search box with a magnifying glass, you can use that box to perform a fast search using Windows Search Service.
- Also when a Windows XP, Vista, or 7 client searches for a file on Windows Server 2008, the Windows Search Service is used.
- Having fast client searches is a compelling reason alone for installing the File Services role in Windows Server 2008. This makes users more productive and reduces time using the network that connects to a server.



The Compress Attribute

- A folder and its contents can be stored on the disk in a compressed format, which is an option that enables you to reduce the amount of disk space used for files. This is particularly useful in situation in which disk space is limited or for folders that are accessed infrequently.
- Compression saves space and a user can work on a compressed file in the same manner as an uncompressed one.
- The disadvantage of compressed files is increased CPU overhead to open the files and to copy them. On a busy server, this can be a serious consideration. Furthermore, you cannot execute a compressed program file.



The Compress Attribute

- When you compress a folder, you have the option to compress the folder, its subfolders, and files in the folder.
- When you add new files to a folder marked with the compress attribute, the new files are compressed automatically.
- By default, compressed files and folders are displayed in colored font, such as blue. If they are not displayed in color, you can turn this feature on.

WARNING

If you are concerned with security and want to use the encrypt attribute, do not compress files because compressed files cannot be encrypted.



The Encrypt Attribute

- The NTFS encrypt attribute protects folders and files so that only the user who encrypts the folder or file is able to read it.
- As a server administrator, you might use this option to protect certain system files or new software files that you are not ready to release for general use.
- In an organization with sensitive file contents, encryption can be an essential security measure.
- It is also good business practice to encrypt stored files vital to business strategy or containing company secrets.



The Encrypt Attribute

- An encrypted folder or file uses the Microsoft Encrypting File System (EFS) which sets up a unique private encryption key associated with the user account that encrypted the folder or file.
- The file is protected from network intruders and in situations in which a server or hard drive is stolen.
- EFS uses both symmetric and asymmetric encryption techniques.
- The symmetric portion uses a single key to encrypt the file or folder.
- In the asymmetric portion, two encryption keys are used to protect the key for encrypting the file or folder. Because the asymmetric portion is connected to a user account, the account should have a strong password to help ensure that attackers can't guess it easily.



Dynamic Volume Management

- Dynamic Volume Management enables you to create, change, or mirror volumes without rebooting, by using dynamic storage and disks.
- A dynamic disk has a single partition within which you can create volumes.



Player | [Icons]

Server Manager

File Action View Help

Server Manager (TESTBEDSERVER)

- Roles
- Features
- Diagnostics
- Configuration
- Storage
 - Windows Server Backup
 - Disk Management**

Disk Management Volume List + Graphical View

Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primary Pa

Disk 0
Basic
40.00 GB
Online

CD-ROM 0
DVD (D:)
No Media

■ Unallocated ■ Primary partition

Actions

Disk Management

- More Actions
 - Refresh
 - Rescan Disks
 - All Tasks ▶
 - View ▶
 - Help

Displays Help for the current selection.

Start | [Icons] | Server Manager | [Icons] | 1:29 PM



Distributed File System (DFS)

- The Distributed File System (DFS) provides for the creation of a directory, called a namespace, that spans several file servers and allows users to easily search and locate files or folders distributed over the network.
- DFS can be either part of a workgroup or an Active Directory domain, wherein spreading the information across several domain controllers provides a degree of fault tolerance..



Player | [Icons] | Server Manager

File Services

Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed
File Replication Service	Not installed
Indexing Service	Not installed

Description:
[File Server](#) manages shared folders and enables users to access files on this computer from the network.

Resources and Support

Last Refresh: 10/2/2013 1:31:53 PM [Configure refresh](#)



Windows Server Backup

- Server 2008 introduced a new backup solution that has been designed specifically for smaller organizations, which is indicated by its redesigned architecture and options for an organization.
- In the early days of backup, you could only back up to tape. Then the capability to backup to media was added, in addition to tape support. Server 2008 allows back up to only media, including DVDs and external drives.
- This is a big shift, and Microsoft's explanation on the removal of tape drive support is that it found that customers who used tapes for back up use third-party back up solutions. So they wanted to better tailor the back up applications to those who use the in-product backup solution: smaller organizations.



Windows Server Backup

- WSB is a feature, which is installed via the Server Manager. There are two subcomponents. The main WSB component contains the core WSB graphical and CLI environments. The Command-Line Tools component contains a script for managing backups via PowerShell.
- This is illustrated on the next slide.



Player ▾ | [Icons] | [Close]

Windows Server Backup [Close] [Min] [Max]

Add Features Wizard

Select Features

Select one or more features to install on this server.

Features:

- Remote Assistance
- Remote Differential Compression
- Remote Server Administration Tools
 - Removable Storage Manager
 - RPC over HTTP Proxy
 - Simple TCP/IP Services
 - SMTP Server
- SNMP Services
 - Storage Manager for SANs
 - Subsystem for UNIX-based Applications
 - Telnet Client
 - Telnet Server
 - TFTP Client
- Windows Internal Database
- Windows PowerShell (Installed)
- Windows Process Activation Service
 - Windows Server Backup Features**
 - Windows Server Backup
 - Command-line Tools
 - Windows System Resource Manager
 - WinRM IIS Extension
 - WMI Service

[More about features](#)

Description:
[Windows Server Backup Features](#) allow you to back up and recover your operating system, applications, and data. You can schedule backups to run once a day or more often, and can protect the entire server or specific volumes.

< Previous Next > Install Cancel

Start | [Icons] | Server Manager | [Icons] | 1:35 PM



Windows Server Backup

- Performing a backup is simple, which is the point behind WSB.
- You must be an administrator or a member of the backup operators group to perform a backup.
- To switch between performing a full or incremental backup, use the Configure Performance Settings action within WSB. Additionally you can select different types of backup for each volume if required. This is shown on the next page.



Player ▾ | [Icons] [?] [?]

Server Manager

File Action View Help

← → [?] [?]

Server Manager (TESTBEDSERVER)

- + Roles
- + Features
- + Diagnostics
- + Configuration
- Storage
- + Windows Server Backup
- + Disk Management

Windows Server Backup

You can perform a single backup or schedule a regular backup using 1

No backup has been configured for this computer. Use Backup Schedule Wizard or Backup Once

Messages

Time	Message	Description

Status

Last Backup

Status: -

Time: -

View details

Next Backup

Status: -

Time: -

View details

Actions

Windows Server Backup

- Backup Schedule...
- Backup Once...
- Recover...
- Configure Performance Settings...
- View ▾
- Help



Player ▾ | [Icons] [?] [?]

Server Manager [?] [?] [?]

File Action View Help

← → [?] [?]

Server Manager (TESTBEDSERVER)

- Roles
- Features
- Diagnostics
- Configuration
- Storage
- Windows Server Backup**
- Disk Management

Windows S

Window

No

Messages

Time

Status

Last Back

Status:

Time:

View c

Optimize Backup Performance [X]

You can optimize backup and server performance by choosing one of the following settings.

- Always perform full backup**
This option slows down the backup speed, but does not impact overall performance.
- Always perform incremental backup**
This option increases the backup speed, but might decrease performance of the volume because shadow copies are left behind. Not recommended for servers with hard disk-intensive applications.
- Custom**
This option enables you to configure each volume separately to either run full backups or incremental backups.

Volume	Backup Option
Local disk (C:)	Full backup ▾

OK Cancel

Actions

Windows Server Backup

- Backup Schedule...
- Backup Once...
- Recover...
- Configure Performance Settings...

View ▾

Help [?]



Player ▾ | [Icons] [Icons] [Icons]


Server Manager

File Action View Help

Server Manager (TESTBEDSERVER)

- Roles
- Features
- Diagnostics
- Configuration
- Storage
- Windows Server Backup**
- Disk Management

Backup Schedule Wizard



Getting started

You can use this wizard to configure backups to run on a regular schedule.

To create a backup schedule, you should first decide:

- What to backup (full server or just certain volumes)
- When and how often to backup
- Where to store the backups (which hard disks)

To continue, click Next.

[More about scheduling backups](#)

< Previous Next > Finish Cancel

Windows Server Backup

- Backup Schedule...
- Backup Once...
- Over...
- Configure Performance Settings...

Start | [Icons] Server Manager | [Icons] 2:15 PM



Backup Schedule Wizard

Select backup configuration

Getting started
Select backup configur...
Specify backup time
Select destination disk
Label destination disk
Confirmation
Summary

What type of configuration do you want to schedule?

- Full Server (recommended)
I want to back up all my server data, applications, and system state.
Backup size: 32.40 GB
- Custom
I want to exclude some volumes from scheduled backups.

[Backing up only the system state of the server using the command line](#)

< Previous Next > Finish Cancel



Backup Schedule Wizard

Specify backup time

Getting started
Select backup configur...
Specify backup time
Select destination disk
Label destination disk
Confirmation
Summary

How often and when do you want to run backups?

Once a day
Select time of day: 9:00 PM

More than once a day
Click an available time and then click Add to add it to the backup schedule.

Available time: Scheduled time:

12:00 AM		9:00 PM
12:30 AM		
1:00 AM		
1:30 AM		
2:00 AM	Add >	
2:30 AM	< Remove	
3:00 AM		
3:30 AM		
4:00 AM		
4:30 AM		

[Learn about advanced scheduling options using the command line](#)

< Previous Next > Finish Cancel

