Lesson 17: Maintaining Active Directory

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 5.3: Maintain Active Directory
- Automating User Account Management
- Backing Up and Restoring Active Directory
- Configuring Active Directory Snapshots
- Performing Object- and Container-Level Recovery
- Managing Active Directory Offline
- Optimizing an Active Directory Database
- Cleaning Up Metadata

Automating User Account Management

Lesson 17: Maintaining Active Directory

Tools for Importing and Exporting Objects

Regarding Active Directory, to import or export many objects at once, use:

- **CSVDE.exe**: Imports or exports Active Directory Domain Services (AD DS) objects to or from a comma-delimited text file.
- **LDIFDE.exe**: Imports or exports Active Directory objects, including users.

CSVDE.exe

To export all objects in your Active Directory domain:

```
   csvde -f filename
```

To list users or computers or only users with a certain attribute, use these parameters:

- `-i`: Turn on Import mode (The default is Export.)
- `-f` *`filename`*: Input or output filename.
- `-s` *`servername`*: The server to bind to. (The default is a DC of computer's domain.)
- `-t` *`portnum`*: Port number. (The default is 389.)

CSVDE.exe

Options when exporting information:

- `-l list`: List of attributes (comma-separated) to look for in an LDAP search.
- `-o list`: List of attributes (comma separated) to omit from input.
- `-k`: The import goes on, ignoring Constraint Violation and Object Already Exists errors.

CSVDE.exe

To import, from a .csv file, use something like:

```
csvde -i -f filename -k
```

- You cannot use CSVDE to import passwords.
- The account is initially disabled.
- After you reset the password, you can enable the object in AD DS.

CSVDE.exe Example

To export a list of user accounts:

```
csvde -s server1 -f c:\ADUsers.csv -r
"(&(objectClass=user)
(objectCategory=person)
(!userAccountControl=514)" -d
"OU= DC=corporate,dc=contoso,dc=com" -l
cn,SamAccountName,Distinguishname,department,
description,physicalDeliveryOfficeName,
title,manager,telephoneNumber,mobile,
ipPhone,mail
```

LDIFDE.exe

- The LDIFDE command implements batch operations by using LDIF files.
- The LDIF file format consists of a block of lines, which together constitute a single operation.
- Multiple operations in a single file are separated by a blank line.

LDIFDE.exe

The contents of the LDIF file look similar to this:

```
dn: CN=John Smith,OU=Sales,OU=User Accounts,DC=contoso,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: John Smith
sn: Smith
title: Sales Manager
description: Sales Team Manager
givenName: John
displayName: Smith, John
company: Contoso Corp
sAMAccountName: john.smith
userPrincipalName: john.smith@contoso.com
mail: john.smith@contoso.com
```

LDIFDE.exe

To import an LDIF file called *NewUsers.ldf*, you use:

```
ldifde -i -f C:\NewUsers.ldf -k
```

Backing Up and Restoring Active Directory

Lesson 17: Maintaining Active Directory

Backups

A ***backup*** or the process of backing up refers to making copies of data so that these additional copies can be used to restore the original after a data-loss event.

Backup Media

- Magnetic Tape
- Hard Disks
- CDs/DVDs
- Cloud

Understanding the Active Directory Database

The Active Directory database is stored in Active Directory database file (C:\Windows\NTDS\Ntds.dit) and its associated log and temporary files. It includes:

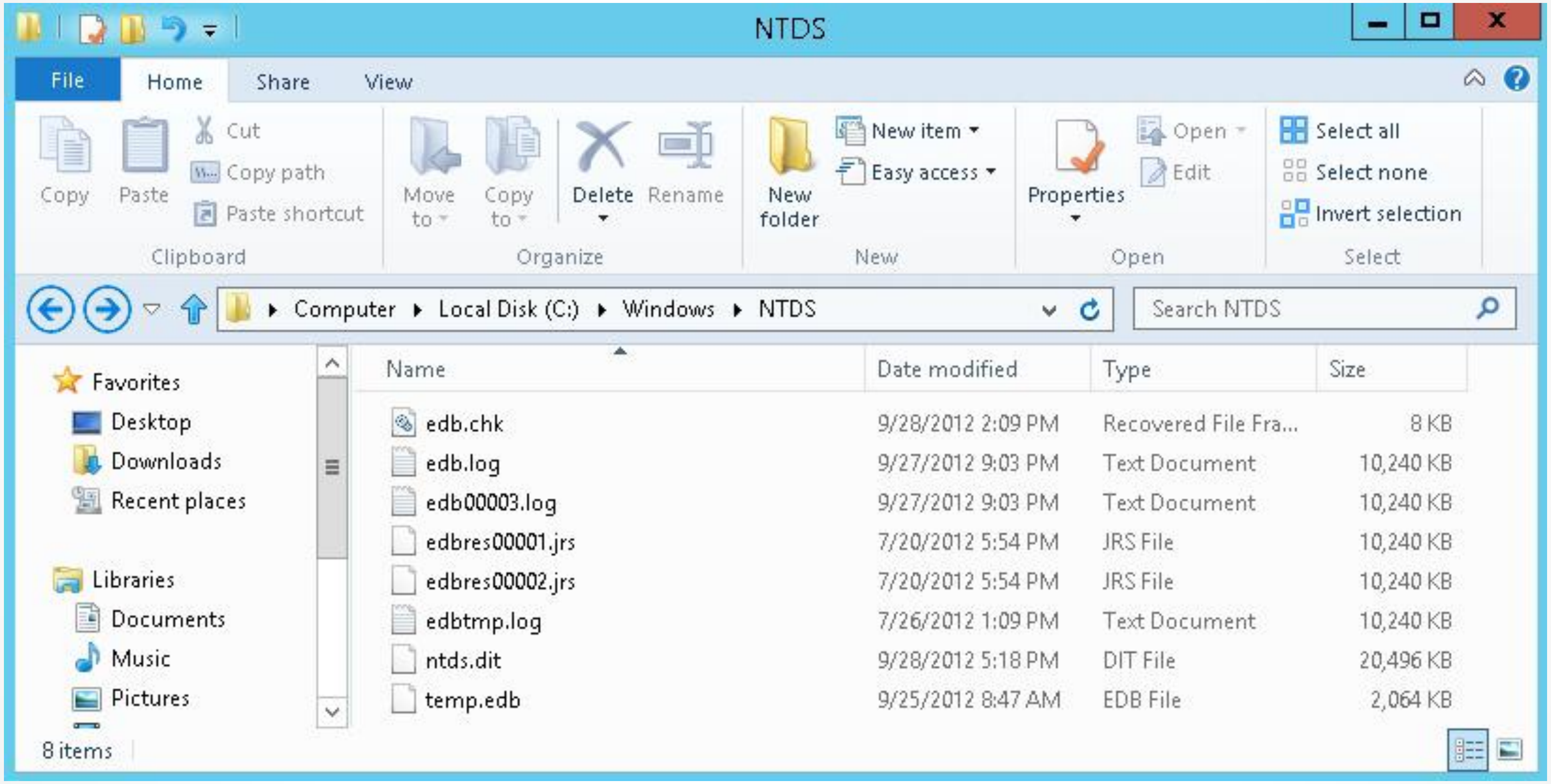
- **Ntds.dit**: The physical database file in which all directory data is stored.
  - Consists of three internal tables: the data table, link table, and security descriptor (SD) table.
  - Contains the schema information, configuration information, and domain information.
- **Edb.log**: The log file into which directory transactions are written before being committed to the database file.
  - Transaction log files used by ESE are 10 MB in size.

Understanding the Active Directory Database

The Active Directory database includes (continued):

- **Edb.chk**: The file used to track the point up to which transactions in the log file have been committed.
- **Res1.log and Res2.log**: Files used to reserve space for additional log files if edb.log becomes full.
- **Temp.edb**: A file used as a scratch pad to store information about in-progress large transactions and to hold pages pulled out of Ntds.dit during maintenance operations.

Understanding the Active Directory Database



Name	Date modified	Type	Size
edb.chk	9/28/2012 2:09 PM	Recovered File Fra...	8 KB
edb.log	9/27/2012 9:03 PM	Text Document	10,240 KB
edb00003.log	9/27/2012 9:03 PM	Text Document	10,240 KB
edbres00001.jrs	7/20/2012 5:54 PM	JRS File	10,240 KB
edbres00002.jrs	7/20/2012 5:54 PM	JRS File	10,240 KB
edbtmp.log	7/26/2012 1:09 PM	Text Document	10,240 KB
ntds.dit	9/28/2012 5:18 PM	DIT File	20,496 KB
temp.edb	9/25/2012 8:47 AM	EDB File	2,064 KB

Looking at the Active Directory database

Understanding the System State

The Windows ***system state*** is a collection of system components that are not contained in a simple file but can be backed up easily.

The Windows system state includes:

- Boot files (such as bootmgr)
- DLL cache folder
- Registry (including COM settings)
- SYSVOL (Group Policy and logon scripts)

Understanding the System State

The Windows system state includes (continued):

- Active Directory NTDS.DIT (domain controllers)
- Certificate Store (if the service is installed)
- User profiles
- COM+ and WMI information
- Cluster service information
- IIS metabase
- System files under Windows Resource Protection

Understanding SYSVOL

The ***SYSVOL*** is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain.

The SYSVOL folder on a domain controller contains:

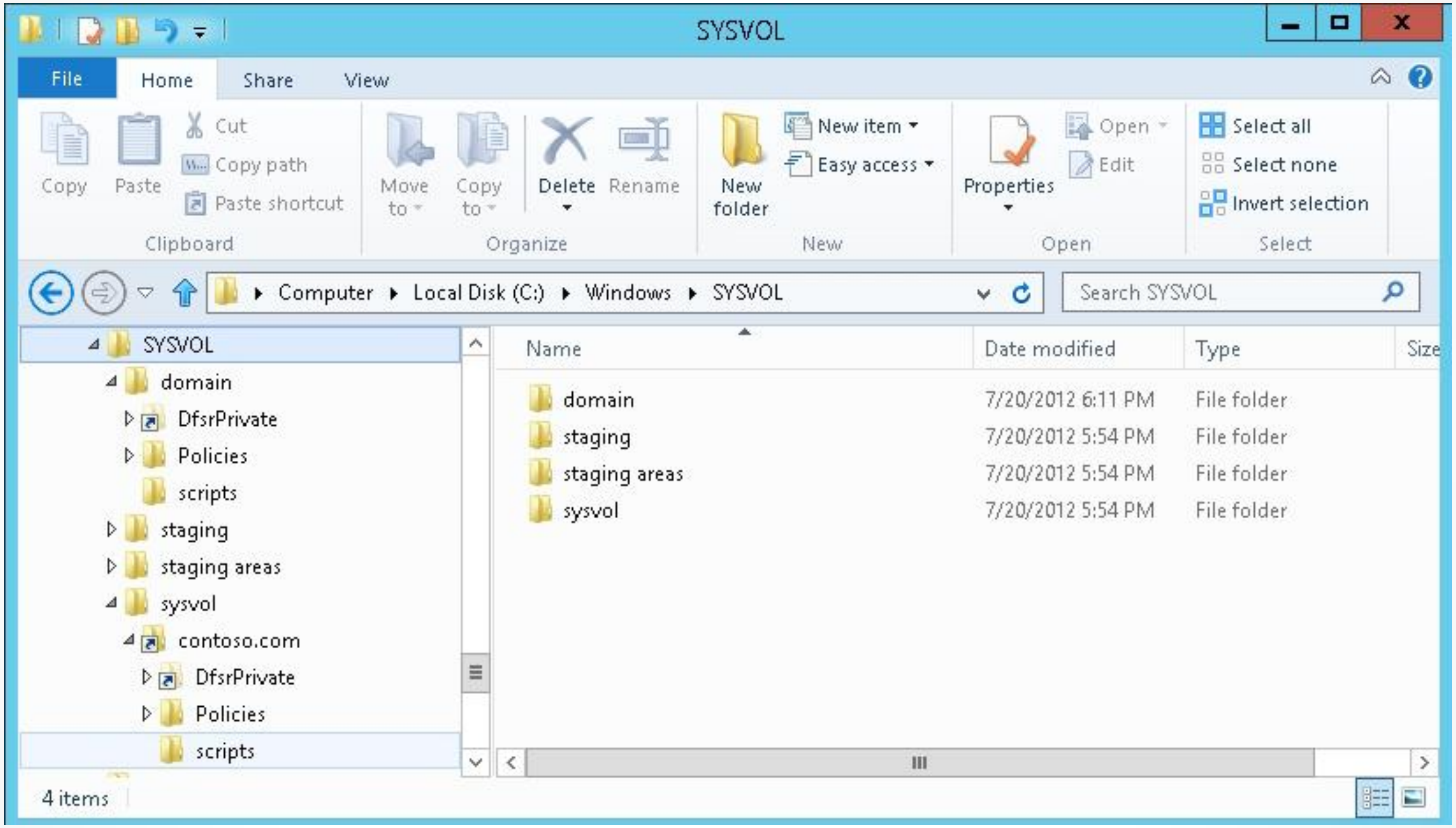
- **Login scripts**: Stores the logon scripts administrated from Active Directory Users and Computers and group policies.
- **Windows Group Policy**: Configuration settings that control the working environment of user and computer accounts and that provide the centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.

Understanding SYSVOL

The SYSVOL folder on a domain controller contains (continued):

- **Distributed File System (DFS) staging folder and files**: Used to synchronize data and files between domain controllers.
- **File system junctions**: A physical location on a hard disk that points to data that is located elsewhere on your disk or other storage device to manage a single instance stored.

Understanding SYSVOL



- SYSVOL
  - domain
    - DfsrPrivate
    - Policies
    - scripts
  - staging
  - staging areas
  - sysvol
    - contoso.com
      - DfsrPrivate
      - Policies
      - scripts

Name	Date modified	Type	Size
domain	7/20/2012 6:11 PM	File folder	
staging	7/20/2012 5:54 PM	File folder	
staging areas	7/20/2012 5:54 PM	File folder	
sysvol	7/20/2012 5:54 PM	File folder	

Looking at the SYSVOL folder

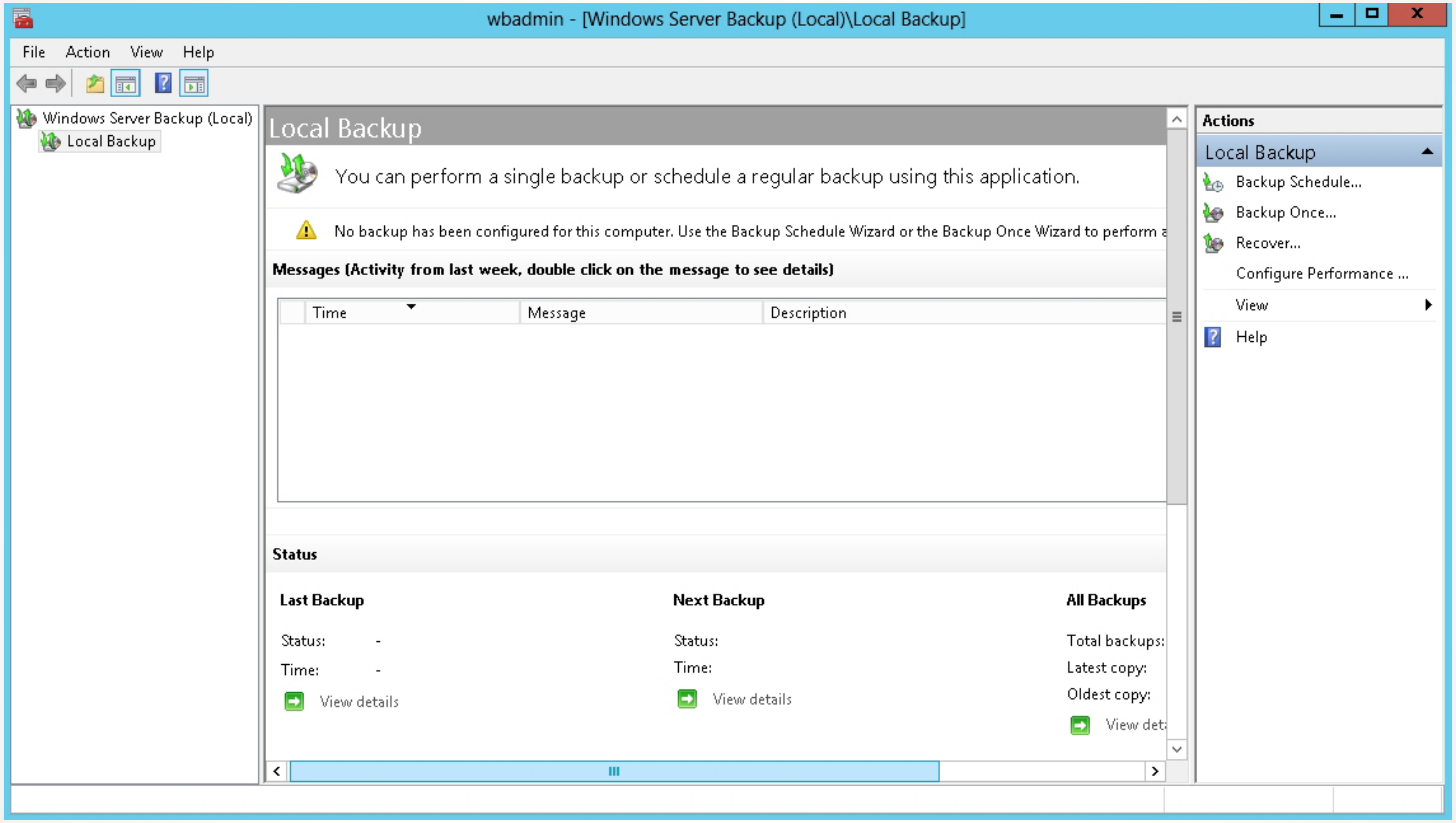
Using Windows Backup

- ***Microsoft Windows Backup*** allows you to back up a system.
- To access the backup and recovery tools for Windows Server 2012 install the Windows Server Backup feature using the Add Roles and Features Wizard.
- To run the Windows Server Backup, you must be a member of the Backup Operators or Administrators group.
- Create a backup using the Backup Schedule Wizard or by using the Backup Once option. You can back up to any local drive or to a shared folder on another server.
- Perform a backup using `wbadmin.exe`, which is the Backup command-line tool.

Performing a Backup of Active Directory and SYSVOL

- You can create a backup using the Backup Schedule Wizard or by using the Backup Once option.
- You can back up to any removable local drive or to a shared folder on another server.

Perform a Backup of the System State Including Active Directory


wbadmin - [Windows Server Backup (Local)\Local Backup]
File
Action
View
Help
Windows Server Backup (Local)
Local Backup
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance ...
View
Help

Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard to perform a

Messages (Activity from last week, double click on the message to see details)

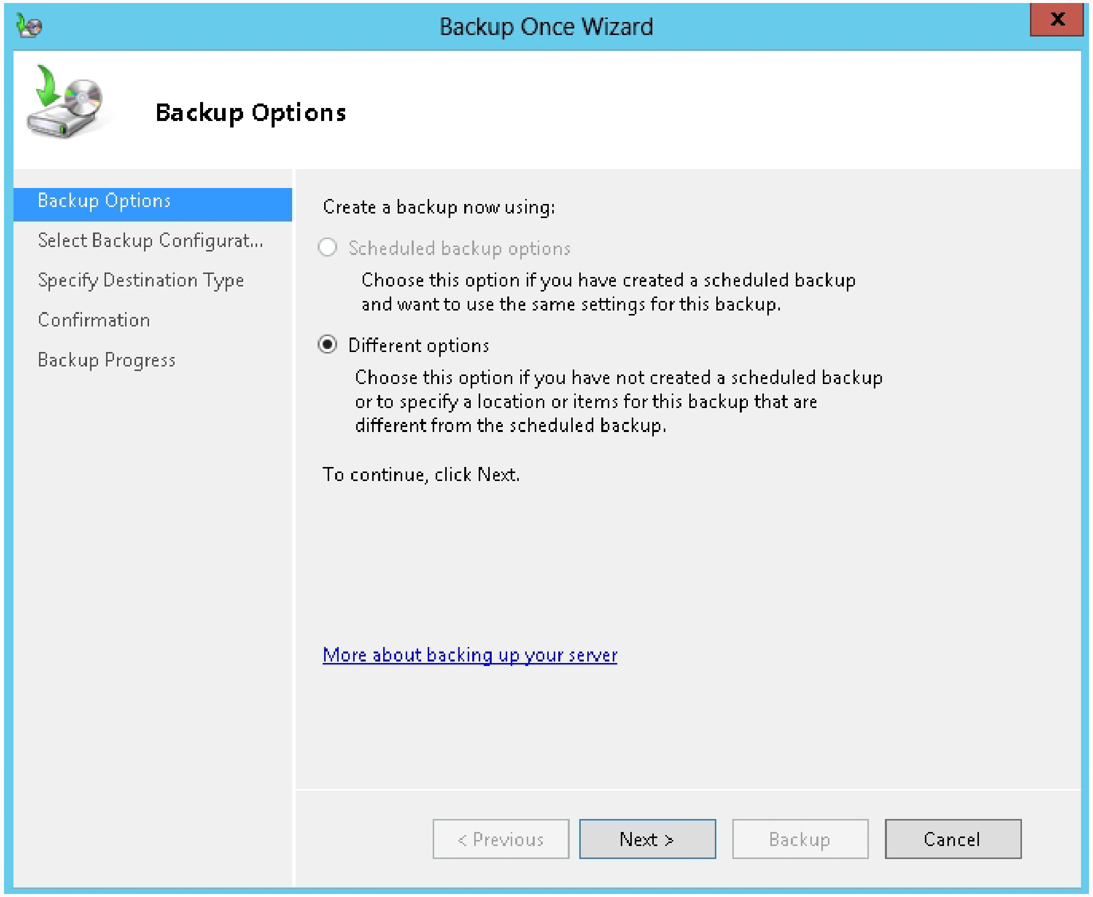
Time	Message	Description

Status

Last Backup	Next Backup	All Backups
Status: -	Status:	Total backups:
Time: -	Time:	Latest copy:
View details	View details	Oldest copy:
		View det

Starting Windows Server Backup

Perform a Backup of the System State Including Active Directory



Create a backup now using:

○ Scheduled backup options

Choose this option if you have created a scheduled backup and want to use the same settings for this backup.

● Different options

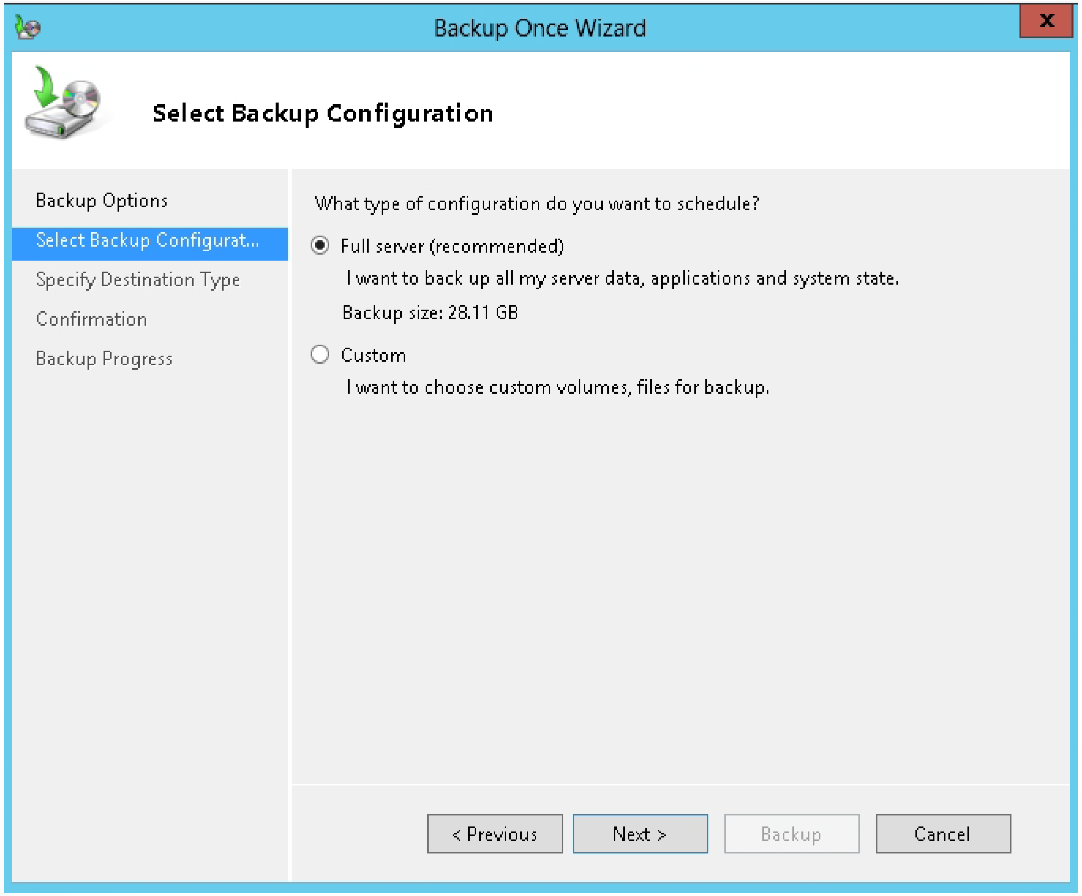
Choose this option if you have not created a scheduled backup or to specify a location or items for this backup that are different from the scheduled backup.

To continue, click Next.

More about backing up your server

Selecting different options

Perform a Backup of the System State Including Active Directory



Select Backup Configuration

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.

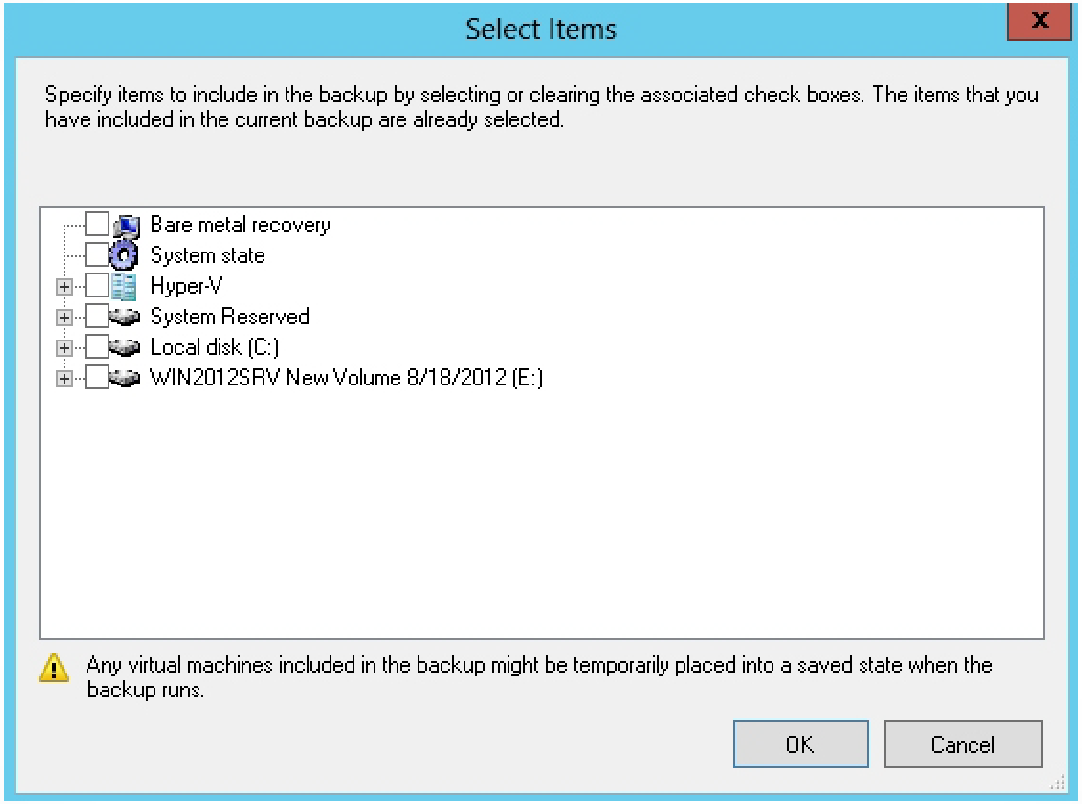
Backup size: 28.11 GB

○ Custom

I want to choose custom volumes, files for backup.

Selecting the backup configuration

Perform a Backup of the System State Including Active Directory



Select Items

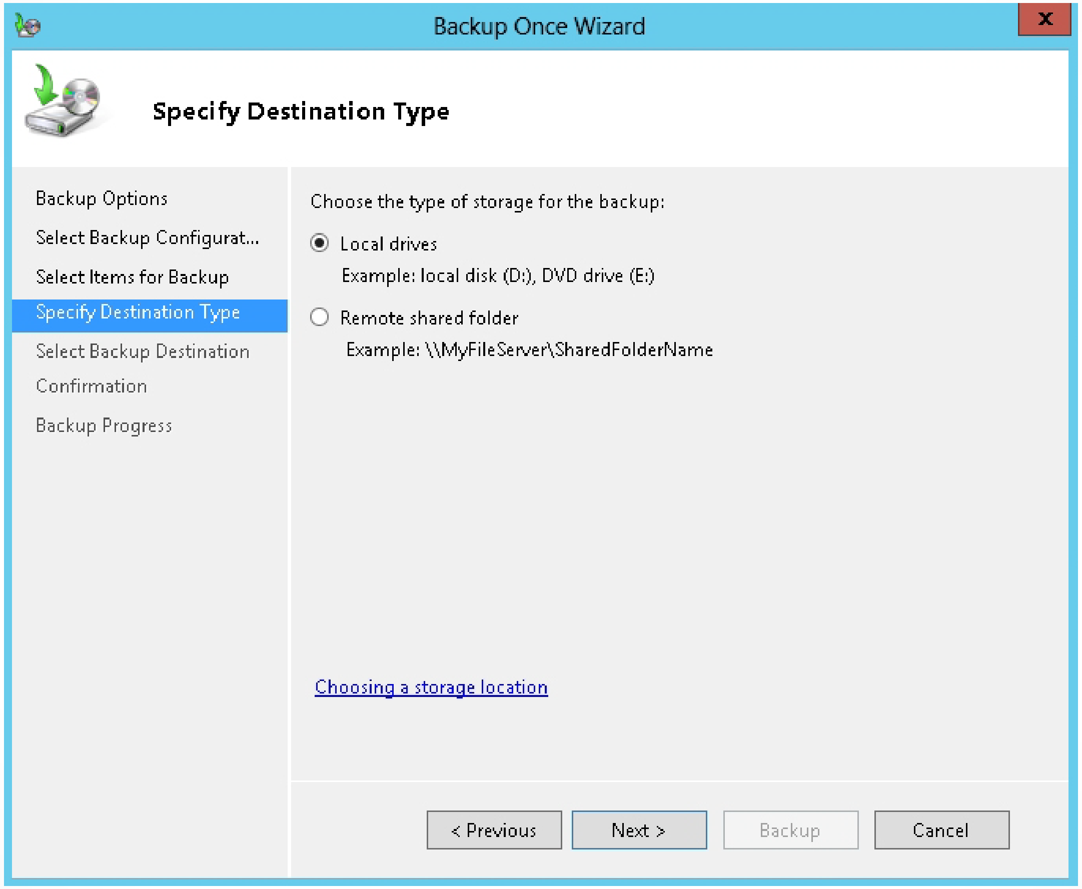
Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

- □ Bare metal recovery
- □ System state
- ⊞ □ Hyper-V
- ⊞ □ System Reserved
- ⊞ □ Local disk (C:)
- ⊞ □ WIN2012SRV New Volume 8/18/2012 (E:)

⚠ Any virtual machines included in the backup might be temporarily placed into a saved state when the backup runs.

Selecting backup items

Perform a Backup of the System State Including Active Directory



Backup Once Wizard

Specify Destination Type

Choose the type of storage for the backup:

● Local drives

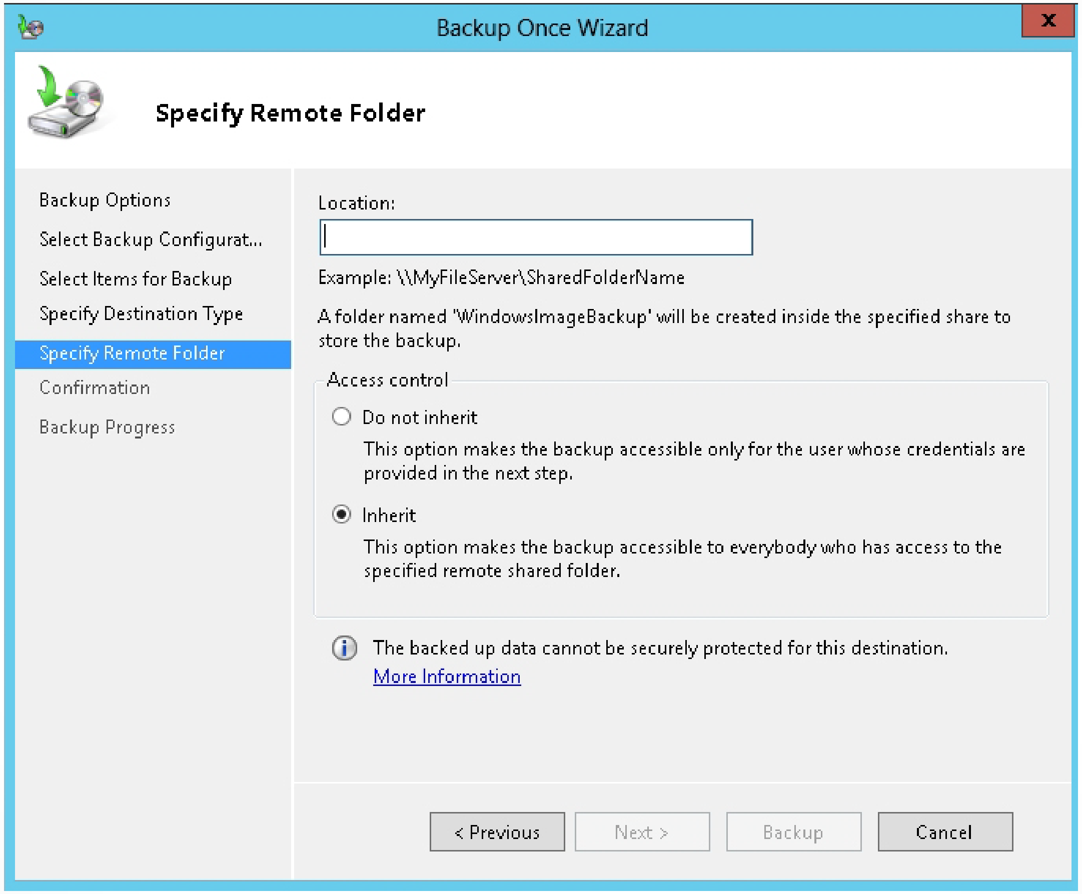
Example: local disk (D:), DVD drive (E:)

○ Remote shared folder

Example: \\MyFileServer\SharedFolderName

Specifying destination type

Perform a Backup of the System State Including Active Directory



Specify Remote Folder

Location:

Example: \\MyFileServer\SharedFolderName

A folder named 'WindowsImageBackup' will be created inside the specified share to store the backup.

Access control

○ Do not inherit

This option makes the backup accessible only for the user whose credentials are provided in the next step.

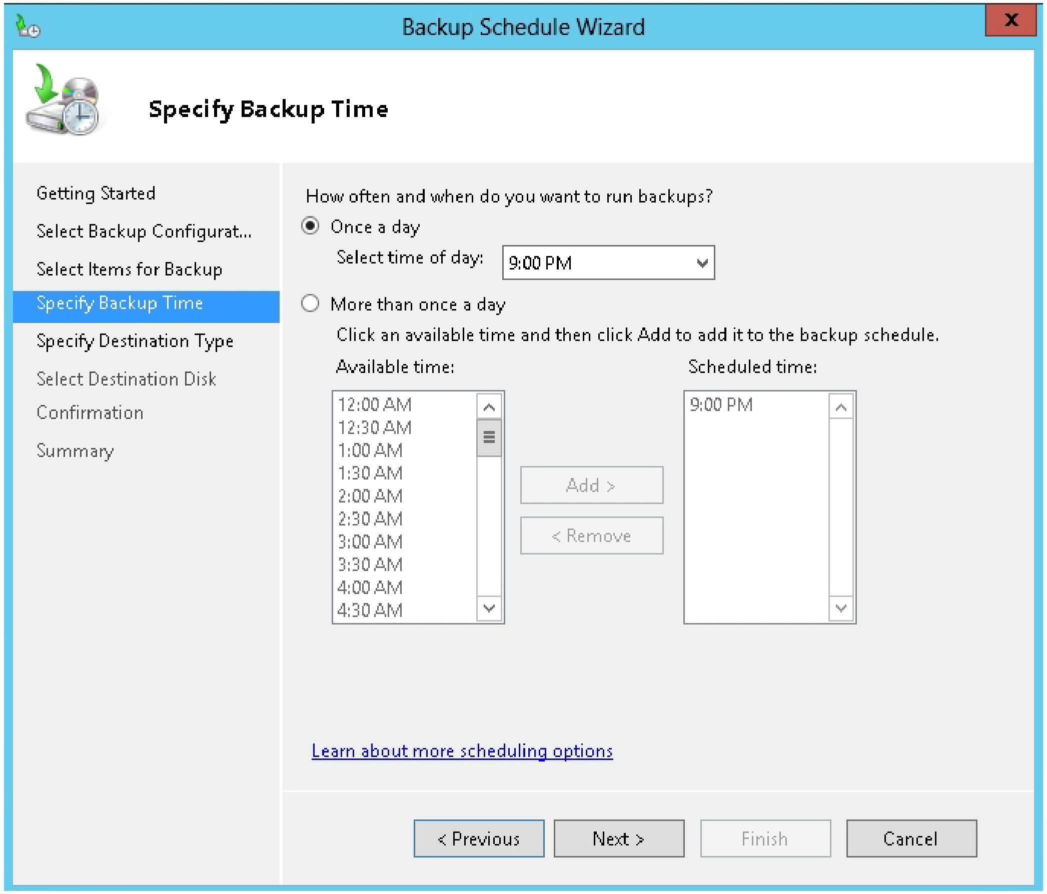
● Inherit

This option makes the backup accessible to everybody who has access to the specified remote shared folder.

The backed up data cannot be securely protected for this destination.

Specifying remote folder

Schedule a Backup of the System State Including Active Directory



Backup Schedule Wizard

Specify Backup Time

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

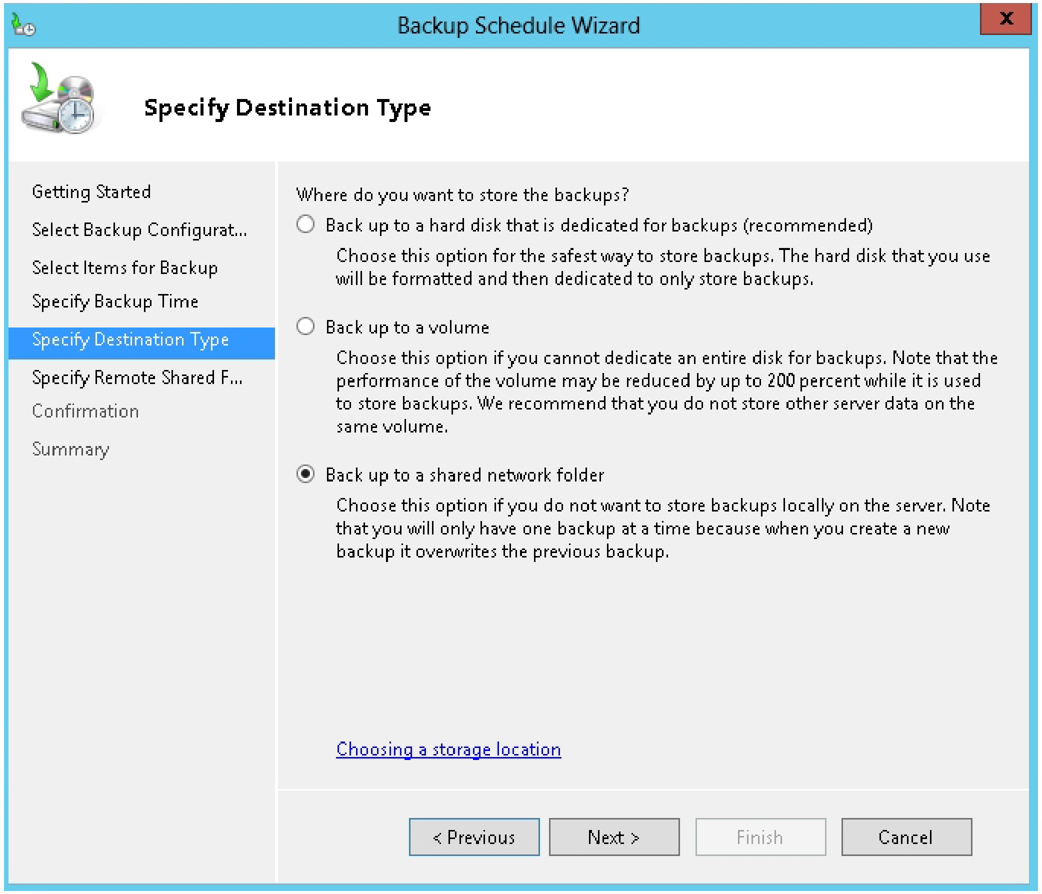
Click an available time and then click Add to add it to the backup schedule.

Available time: 12:00 AM, 12:30 AM, 1:00 AM, 1:30 AM, 2:00 AM, 2:30 AM, 3:00 AM, 3:30 AM, 4:00 AM, 4:30 AM

Scheduled time: 9:00 PM

Specifying when to perform a backup

Schedule a Backup of the System State Including Active Directory



Specify Destination Type

Where do you want to store the backups?

○ Back up to a hard disk that is dedicated for backups (recommended)

Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

○ Back up to a volume

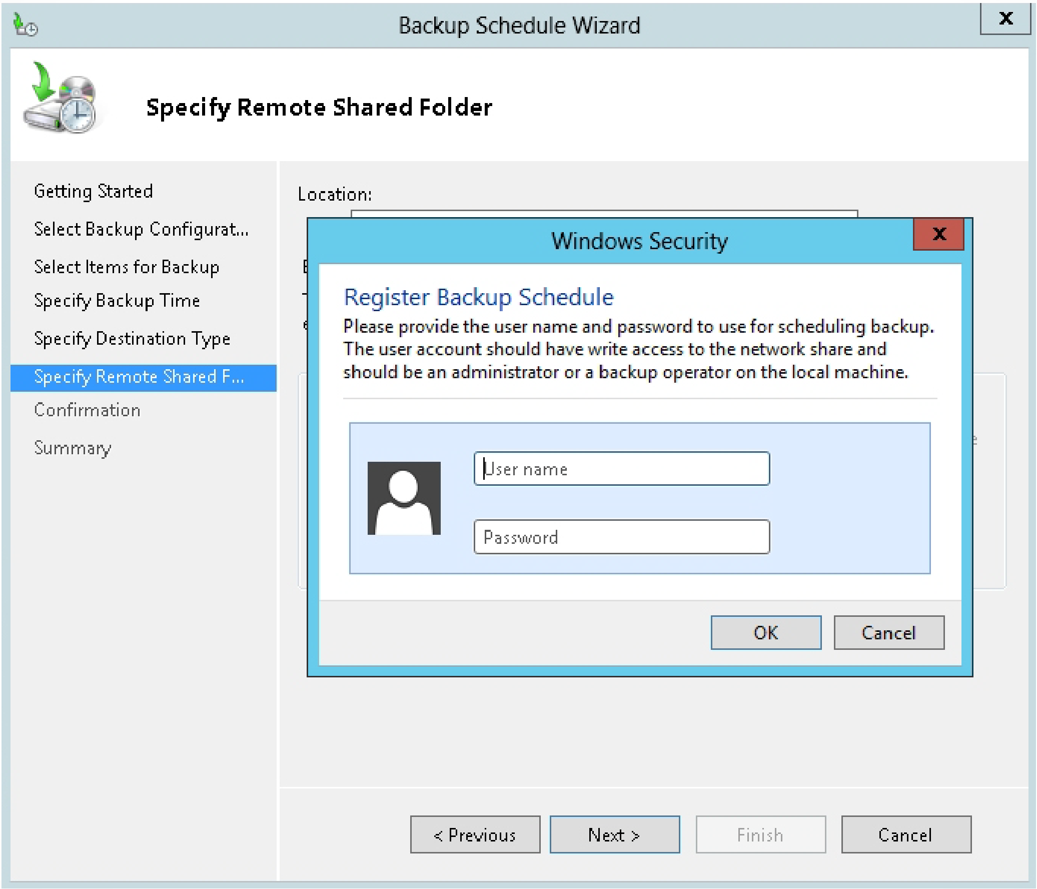
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

● Back up to a shared network folder

Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.

Specifying the destination type

Schedule a Backup of the System State Including Active Directory



Register Backup Schedule

Please provide the user name and password to use for scheduling backup. The user account should have write access to the network share and should be an administrator or a backup operator on the local machine.

Specifying who the backups run under

Performing an Active Directory Restore

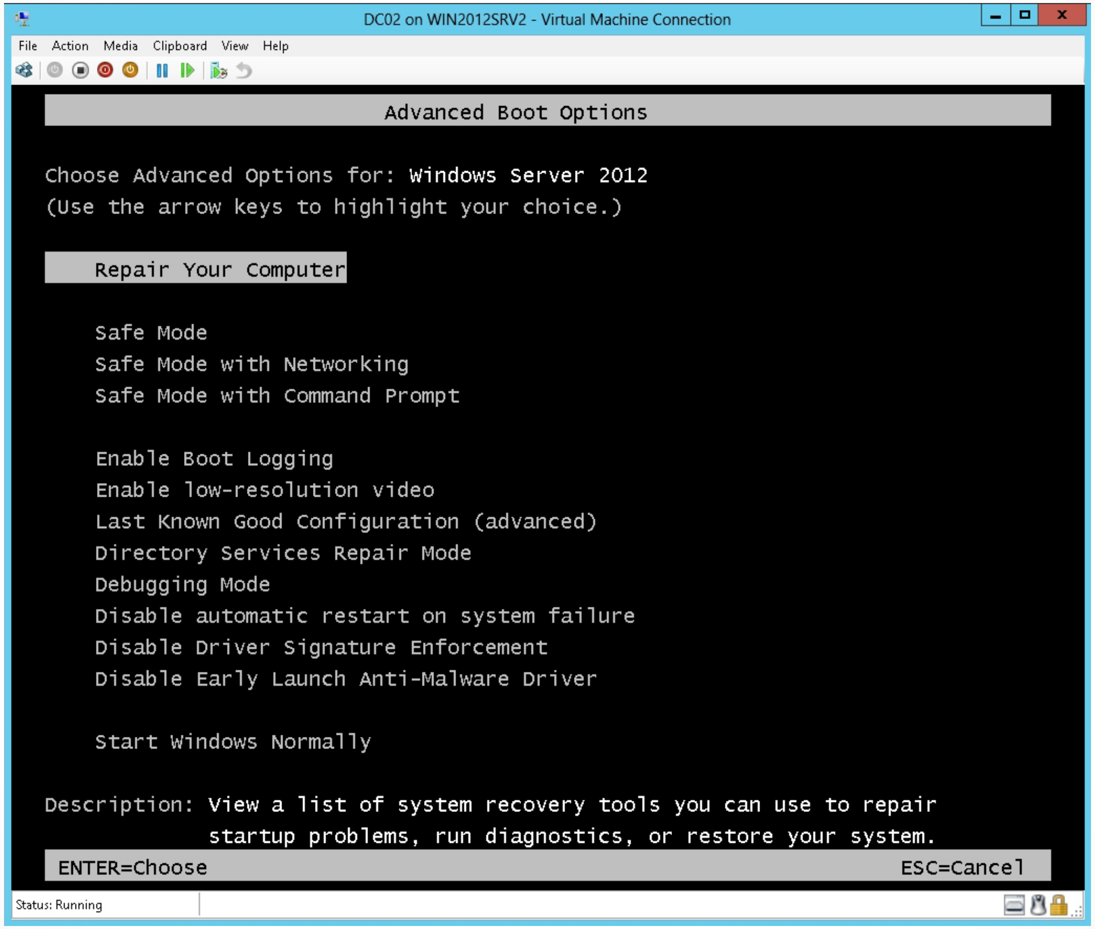
There are two types of restores that you can perform with Active Directory:

- **A nonauthoritative restore**: Restores a backup of Active Directory as of the date of the backup.
- **An authoritative restore**: An override type restore where the information on the restored domain controller is replicated to the other domain controllers.

Performing an Active Directory Restore

- To perform an authoritative restore reboot the computer into the ***Directory Services Restore Mode (DSRM)***, which is a mode of Windows that takes the Active Directory offline.
- Access this mode from the Advanced Boot menu, which is accessed before Windows completes booting by pressing the F8 key.

Perform a Restore of the System State

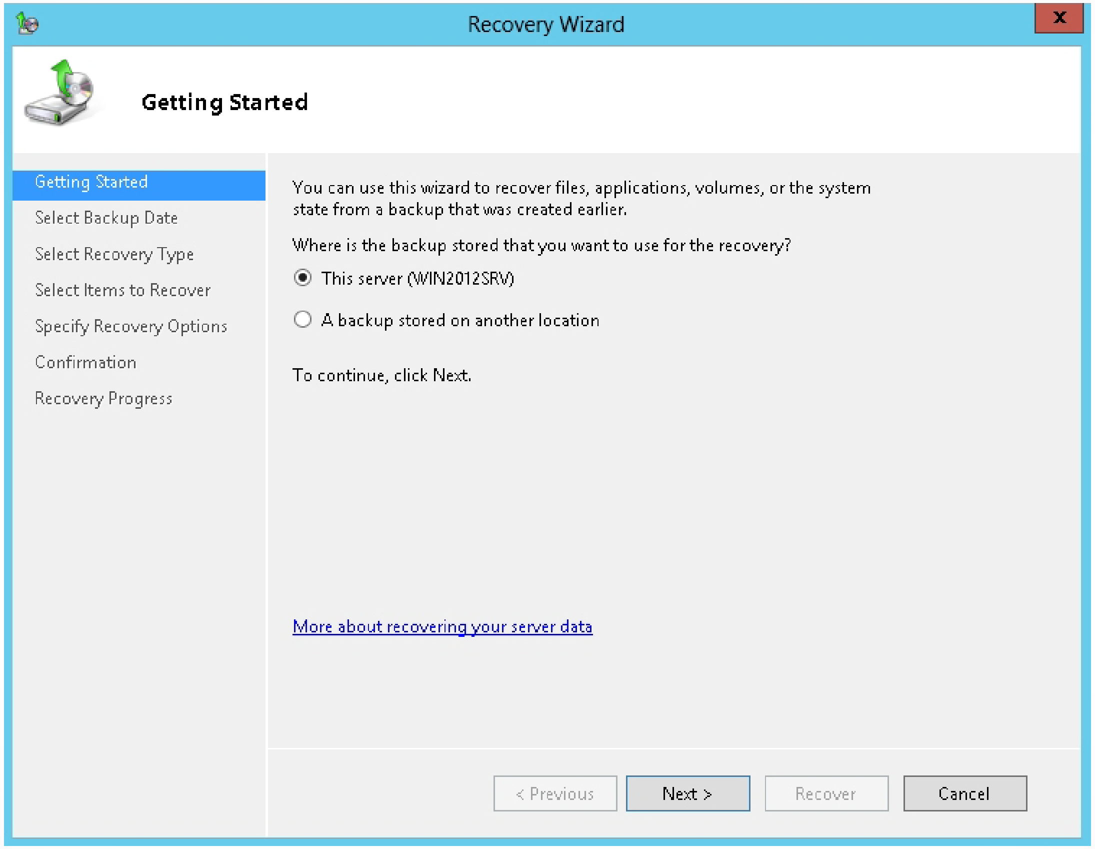


DC02 on WIN2012SRV2 - Virtual Machine Connection
File Action Media Clipboard View Help

```
                        Advanced Boot Options

Choose Advanced Options for: Windows Server 2012
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video
    Last Known Good Configuration (advanced)
    Directory Services Repair Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
    Disable Early Launch Anti-Malware Driver

    Start Windows Normally

Description: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.
ENTER=Choose                                                  ESC=Cancel
```

Accessing the Advanced Boot Options menu

Perform a Restore of the System State



Recovery Wizard

Getting Started

You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.

Where is the backup stored that you want to use for the recovery?

● This server (WIN2012SRV)

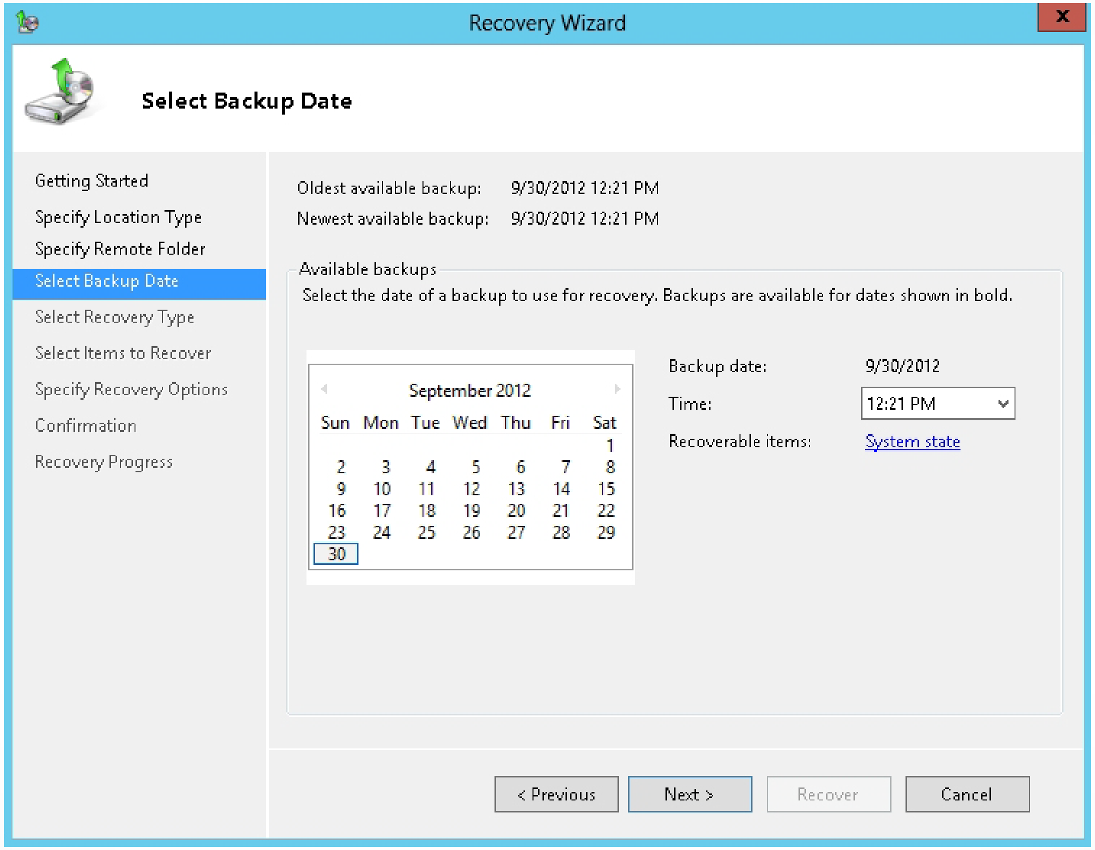
○ A backup stored on another location

To continue, click Next.

More about recovering your server data

Specifying where the backup is located

Perform a Restore of the System State



Select Backup Date

Oldest available backup: 9/30/2012 12:21 PM

Newest available backup: 9/30/2012 12:21 PM

Available backups

Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

September 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

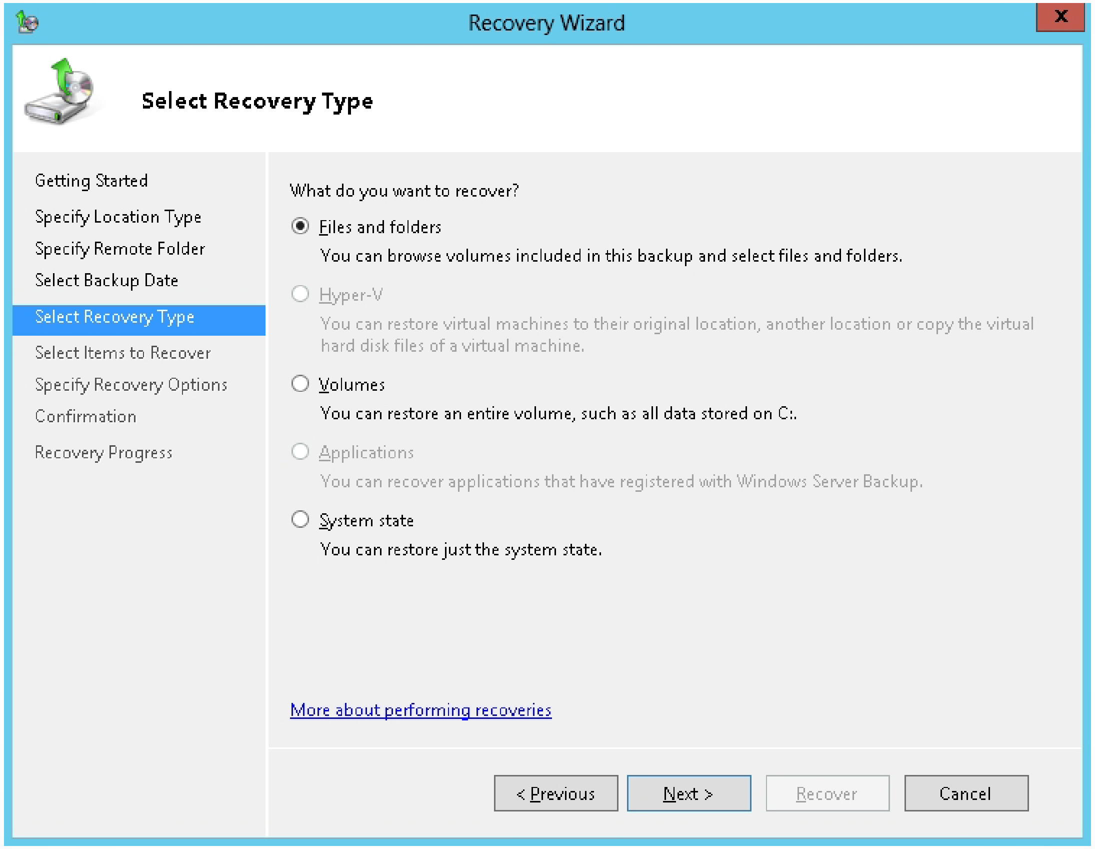
Backup date: 9/30/2012

Time: 12:21 PM

Recoverable items: System state

Selecting the backup date

Perform a Restore of the System State



Recovery Wizard

Select Recovery Type

What do you want to recover?

● Files and folders

You can browse volumes included in this backup and select files and folders.

○ Hyper-V

You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.

○ Volumes

You can restore an entire volume, such as all data stored on C:.

○ Applications

You can recover applications that have registered with Windows Server Backup.

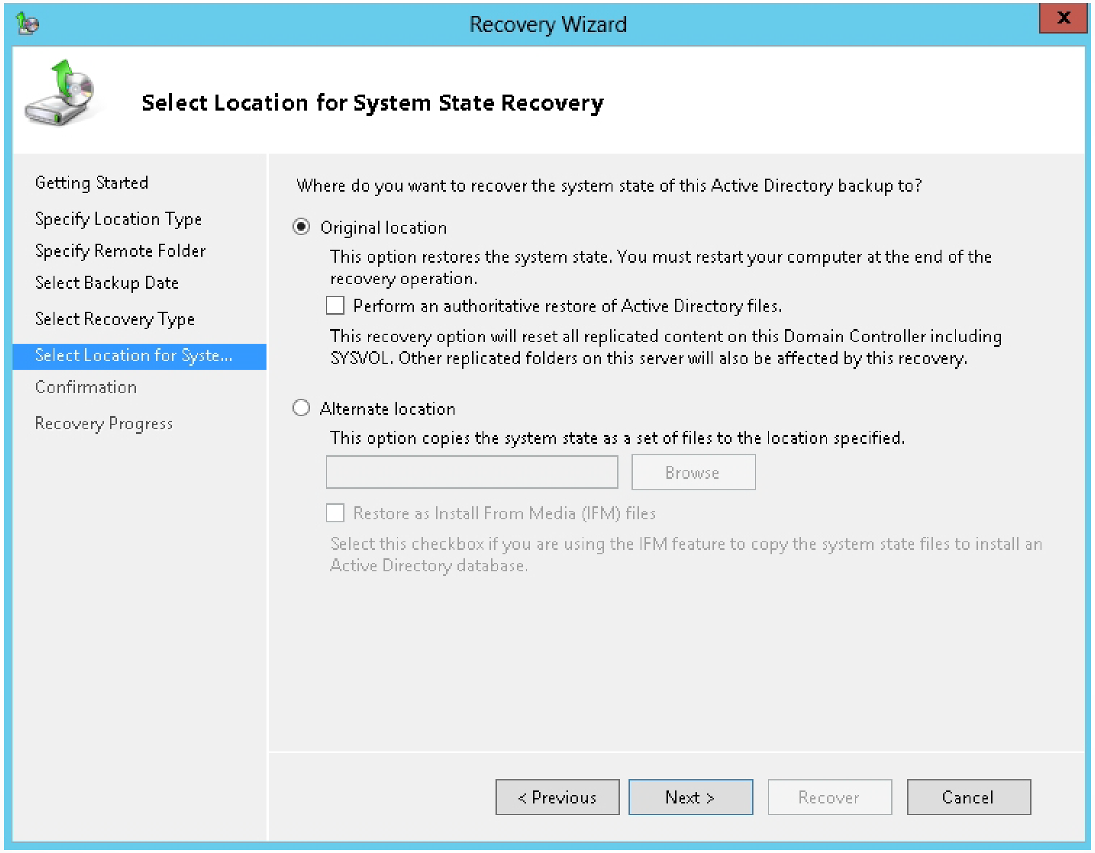
○ System state

You can restore just the system state.

More about performing recoveries

Selecting the recovery type

Perform a Restore of the System State



Select Location for System State Recovery

Where do you want to recover the system state of this Active Directory backup to?

● Original location

This option restores the system state. You must restart your computer at the end of the recovery operation.

□ Perform an authoritative restore of Active Directory files.

This recovery option will reset all replicated content on this Domain Controller including SYSVOL. Other replicated folders on this server will also be affected by this recovery.

○ Alternate location

This option copies the system state as a set of files to the location specified.

□ Restore as Install From Media (IFM) files

Select this checkbox if you are using the IFM feature to copy the system state files to install an Active Directory database.

Selecting the location for system state recovery

Configuring Active Directory Snapshots

Lesson 17: Maintaining Active Directory

Snapshots

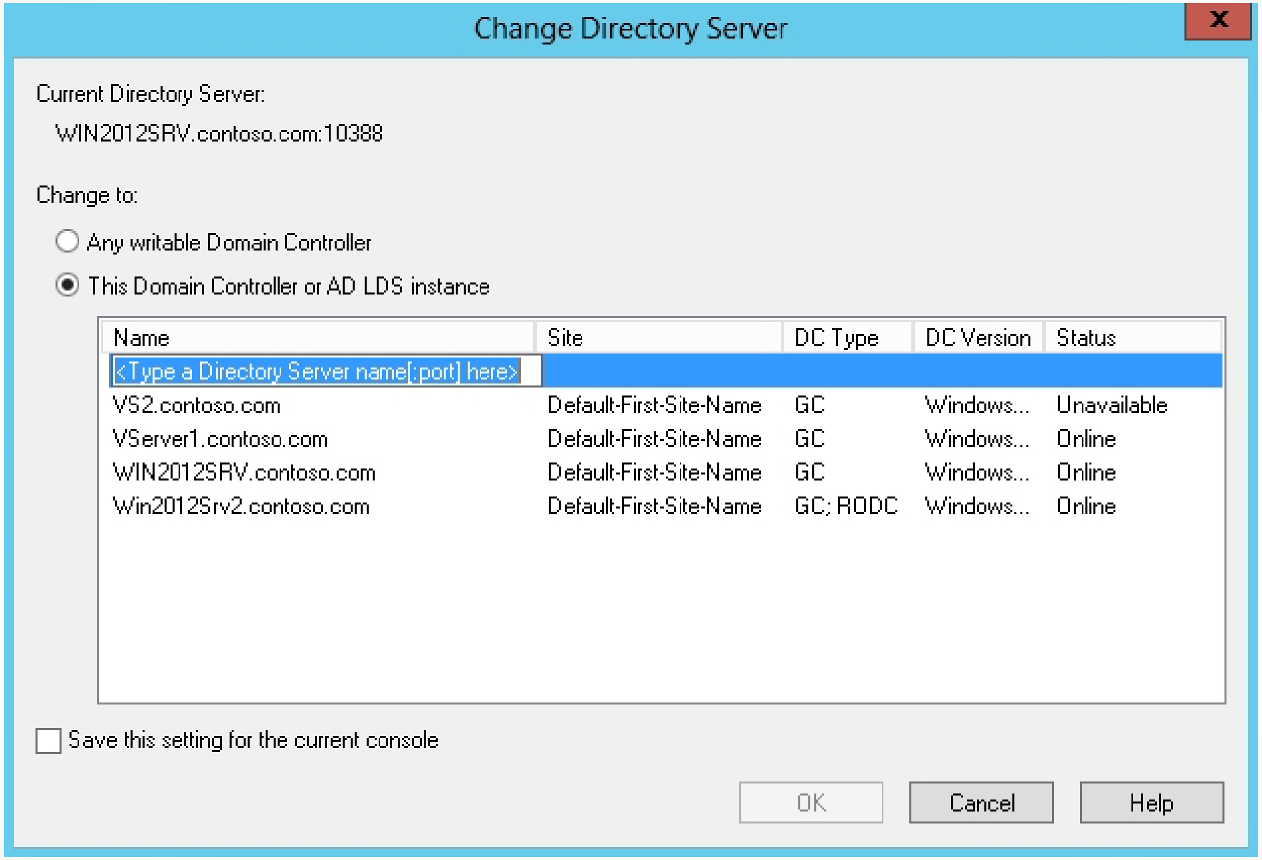
- Another tool used in recovery of Active Directory is the ***Active Directory database mounting tool*** to create and view Active Directory snapshots.
- An ***Active Directory snapshot*** is a shadow copy, created by the Volume Shadow Copy Service (VSS), of the volumes that contain the Active Directory database and log files.

Creating and Using Snapshots

To create and use snapshots:

1. Create a snapshot with `ntdsutil.exe`.
2. Mount the snapshot with the Active Directory database mounting tool.
3. View the objects within the snapshot.
4. When done with the snapshot, dismount the snapshot.

View an AD DS Snapshot



Current Directory Server:

WIN2012SRV.contoso.com:10388

Change to:

○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
VS2.contoso.com	Default-First-Site-Name	GC	Windows...	Unavailable
VServer1.contoso.com	Default-First-Site-Name	GC	Windows...	Online
WIN2012SRV.contoso.com	Default-First-Site-Name	GC	Windows...	Online
Win2012Srv2.contoso.com	Default-First-Site-Name	GC; RODC	Windows...	Online

□ Save this setting for the current console

Specifying the snapshot to view

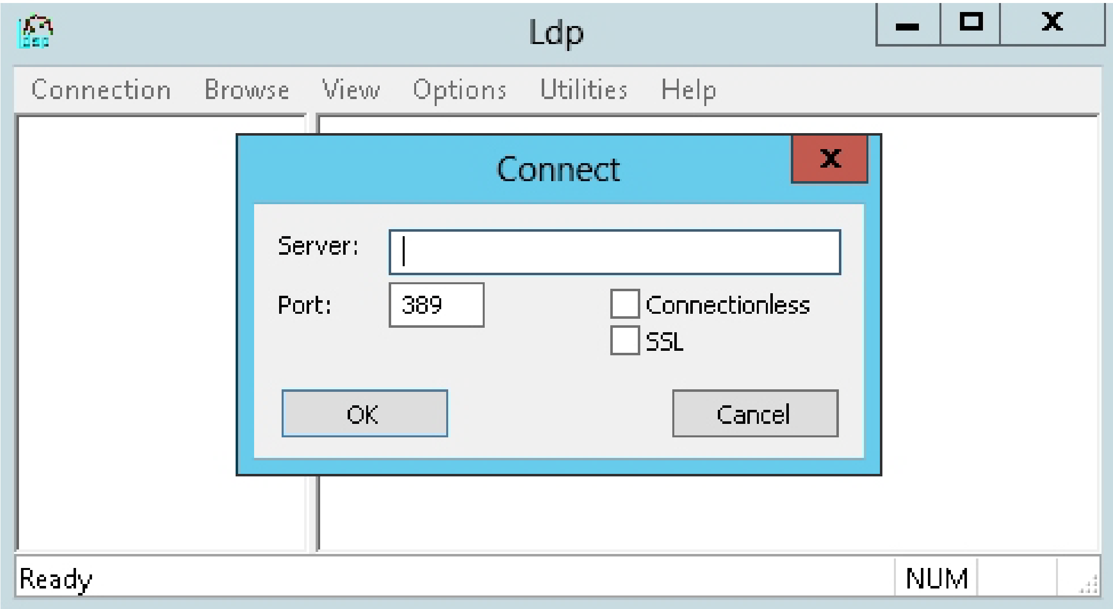
Performing Object- and Container-Level Recovery

Lesson 17: Maintaining Active Directory

Active Directory Recycle Bin

- Starting with Windows Server 2008 R2, Windows offers the Active Directory Recycle Bin.
- The ***Active Directory Recycle Bin*** holds deleted Active Directory containers and objects. You can undelete the items.
- When an object or OU in AD DS is deleted, it is moved to the Deleted Objects container. As long as the object has not been scavenged by the garbage collection process after reaching the end of the object tombstone lifetime, you can restore the deleted object.
- The LDP.exe tool, included with Windows Server 2012, allows users to perform operations against any LDAP-compatible directory, including Active Directory.

Restore a Deleted Object without Using the Recycle Bin



Server:

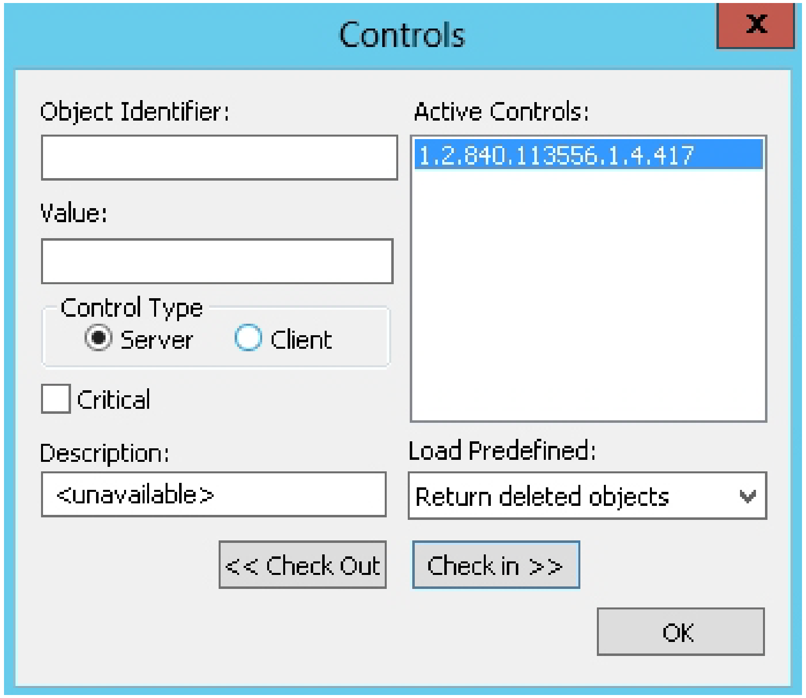
Port: 389

□ Connectionless

□ SSL

Specifying the server to connect to

Restore a Deleted Object Without Using the Recycle Bin



Controls

Object Identifier:

Value:

Control Type
● Server ○ Client

□ Critical

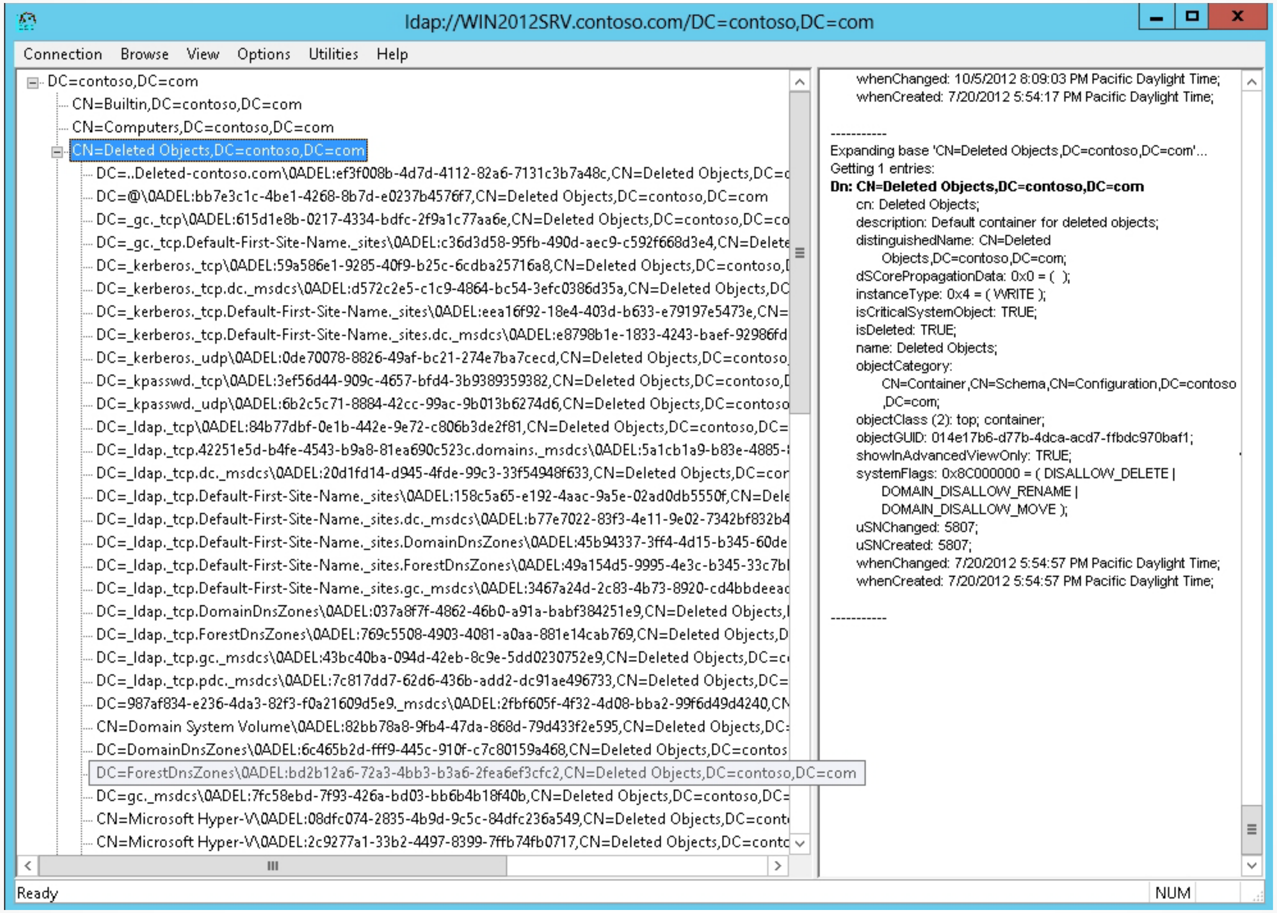
Description: <unavailable>

Active Controls: 1.2.840.113556.1.4.417

Load Predefined: Return deleted objects

Selecting to return deleted objects

Restore a Deleted Object Without Using the Recycle Bin

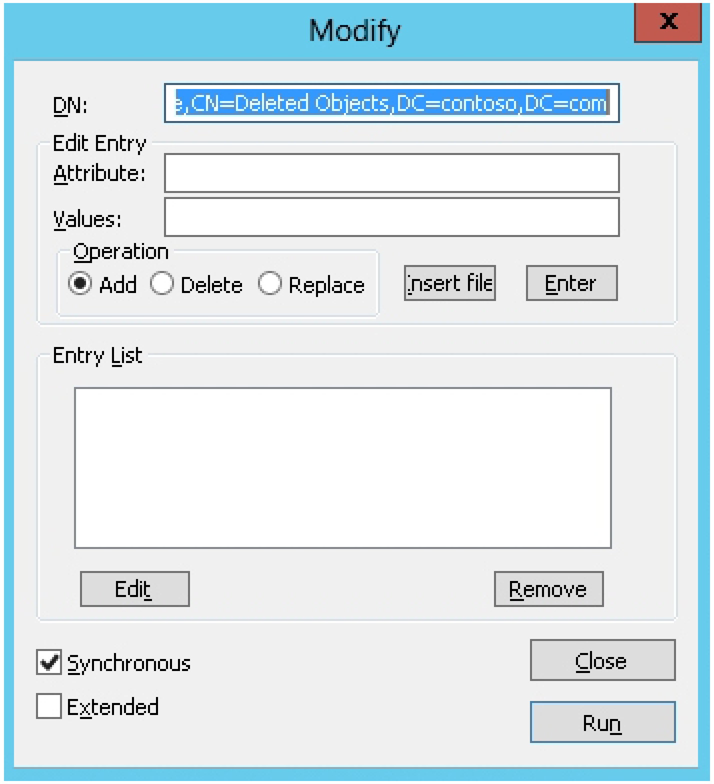


```
DC=contoso,DC=com
    CN=Builtin,DC=contoso,DC=com
    CN=Computers,DC=contoso,DC=com
    CN=Deleted Objects,DC=contoso,DC=com
        DC=..Deleted-contoso.com\0ADEL:ef3f008b-4d7d-4112-82a6-7131c3b7a48c,CN=Deleted Objects,DC=c
        DC=@\0ADEL:bb7e3c1c-4be1-4268-8b7d-e0237b4576f7,CN=Deleted Objects,DC=contoso,DC=com
        DC=_gc._tcp\0ADEL:615d1e8b-0217-4334-bdfc-2f9a1c77aa6e,CN=Deleted Objects,DC=contoso,DC=co
        DC=_gc._tcp.Default-First-Site-Name._sites\0ADEL:c36d3d58-95fb-490d-aec9-c592f668d3e4,CN=Delete
        DC=_kerberos._tcp\0ADEL:59a586e1-9285-40f9-b25c-6cdba25716a8,CN=Deleted Objects,DC=contoso,D
        DC=_kerberos._tcp.dc._msdcs\0ADEL:d572c2e5-c1c9-4864-bc54-3efc0386d35a,CN=Deleted Objects,DC
        DC=_kerberos._tcp.Default-First-Site-Name._sites\0ADEL:eea16f92-18e4-403d-b633-e79197e5473e,CN=
        DC=_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs\0ADEL:e8798b1e-1833-4243-baef-92986fd
        DC=_kerberos._udp\0ADEL:0de70078-8826-49af-bc21-274e7ba7cecd,CN=Deleted Objects,DC=contoso,
        DC=_kpasswd._tcp\0ADEL:3ef56d44-909c-4657-bfd4-3b9389359382,CN=Deleted Objects,DC=contoso,D
        DC=_kpasswd._udp\0ADEL:6b2c5c71-8884-42cc-99ac-9b013b6274d6,CN=Deleted Objects,DC=contoso
        DC=_ldap._tcp\0ADEL:84b77dbf-0e1b-442e-9e72-c806b3de2f81,CN=Deleted Objects,DC=contoso,DC=
        DC=_ldap._tcp.42251e5d-b4fe-4543-b9a8-81ea690c523c.domains._msdcs\0ADEL:5a1cb1a9-b83e-4885-
        DC=_ldap._tcp.dc._msdcs\0ADEL:20d1fd14-d945-4fde-99c3-33f54948f633,CN=Deleted Objects,DC=cor
        DC=_ldap._tcp.Default-First-Site-Name._sites\0ADEL:158c5a65-e192-4aac-9a5e-02ad0db5550f,CN=Dele
        DC=_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs\0ADEL:b77e7022-83f3-4e11-9e02-7342bf832b4
        DC=_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones\0ADEL:45b94337-3ff4-4d15-b345-60de
        DC=_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones\0ADEL:49a154d5-9995-4e3c-b345-33c7b
        DC=_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs\0ADEL:3467a24d-2c83-4b73-8920-cd4bbdeea
        DC=_ldap._tcp.DomainDnsZones\0ADEL:037a8f7f-4862-46b0-a91a-babf384251e9,CN=Deleted Objects,
        DC=_ldap._tcp.ForestDnsZones\0ADEL:769c5508-4903-4081-a0aa-881e14cab769,CN=Deleted Objects,D
        DC=_ldap._tcp.gc._msdcs\0ADEL:43bc40ba-094d-42eb-8c9e-5dd0230752e9,CN=Deleted Objects,DC=c
        DC=_ldap._tcp.pdc._msdcs\0ADEL:7c817dd7-62d6-436b-add2-dc91ae496733,CN=Deleted Objects,DC=
        DC=987af834-e236-4da3-82f3-f0a21609d5e9._msdcs\0ADEL:2fbf605f-4f32-4d08-bba2-99f6d49d4240,CN
        CN=Domain System Volume\0ADEL:82bb78a8-9fb4-47da-868d-79d433f2e595,CN=Deleted Objects,DC=
        DC=DomainDnsZones\0ADEL:6c465b2d-fff9-445c-910f-c7c80159a468,CN=Deleted Objects,DC=contos
        DC=ForestDnsZones\0ADEL:bd2b12a6-72a3-4bb3-b3a6-2fea6ef3cfc2,CN=Deleted Objects,DC=contoso,DC=com
        DC=gc._msdcs\0ADEL:7fc58ebd-7f93-426a-bd03-bb6b4b18f40b,CN=Deleted Objects,DC=contoso,DC=
        CN=Microsoft Hyper-V\0ADEL:08dfc074-2835-4b9d-9c5c-84dfc236a549,CN=Deleted Objects,DC=cont
        CN=Microsoft Hyper-V\0ADEL:2c9277a1-33b2-4497-8399-7ffb74fb0717,CN=Deleted Objects,DC=conto
```

```
    whenChanged: 10/5/2012 8:09:03 PM Pacific Daylight Time;
    whenCreated: 7/20/2012 5:54:17 PM Pacific Daylight Time;

-----------
Expanding base 'CN=Deleted Objects,DC=contoso,DC=com'...
Getting 1 entries:
Dn: CN=Deleted Objects,DC=contoso,DC=com
    cn: Deleted Objects;
    description: Default container for deleted objects;
    distinguishedName: CN=Deleted
        Objects,DC=contoso,DC=com;
    dSCorePropagationData: 0x0 = (  );
    instanceType: 0x4 = ( WRITE );
    isCriticalSystemObject: TRUE;
    isDeleted: TRUE;
    name: Deleted Objects;
    objectCategory:
        CN=Container,CN=Schema,CN=Configuration,DC=contoso
        ,DC=com;
    objectClass (2): top; container;
    objectGUID: 014e17b6-d77b-4dca-acd7-ffbdc970baf1;
    showInAdvancedViewOnly: TRUE;
    systemFlags: 0x8C000000 = ( DISALLOW_DELETE |
        DOMAIN_DISALLOW_RENAME |
        DOMAIN_DISALLOW_MOVE );
    uSNChanged: 5807;
    uSNCreated: 5807;
    whenChanged: 7/20/2012 5:54:57 PM Pacific Daylight Time;
    whenCreated: 7/20/2012 5:54:57 PM Pacific Daylight Time;

-----------
```

Showing deleted objects

Restore a Deleted Object Without Using the Recycle Bin



DN: e,CN=Deleted Objects,DC=contoso,DC=com

Edit Entry

Attribute:

Values:

Operation

● Add ○ Delete ○ Replace

☑ Synchronous

□ Extended

Modifying an object

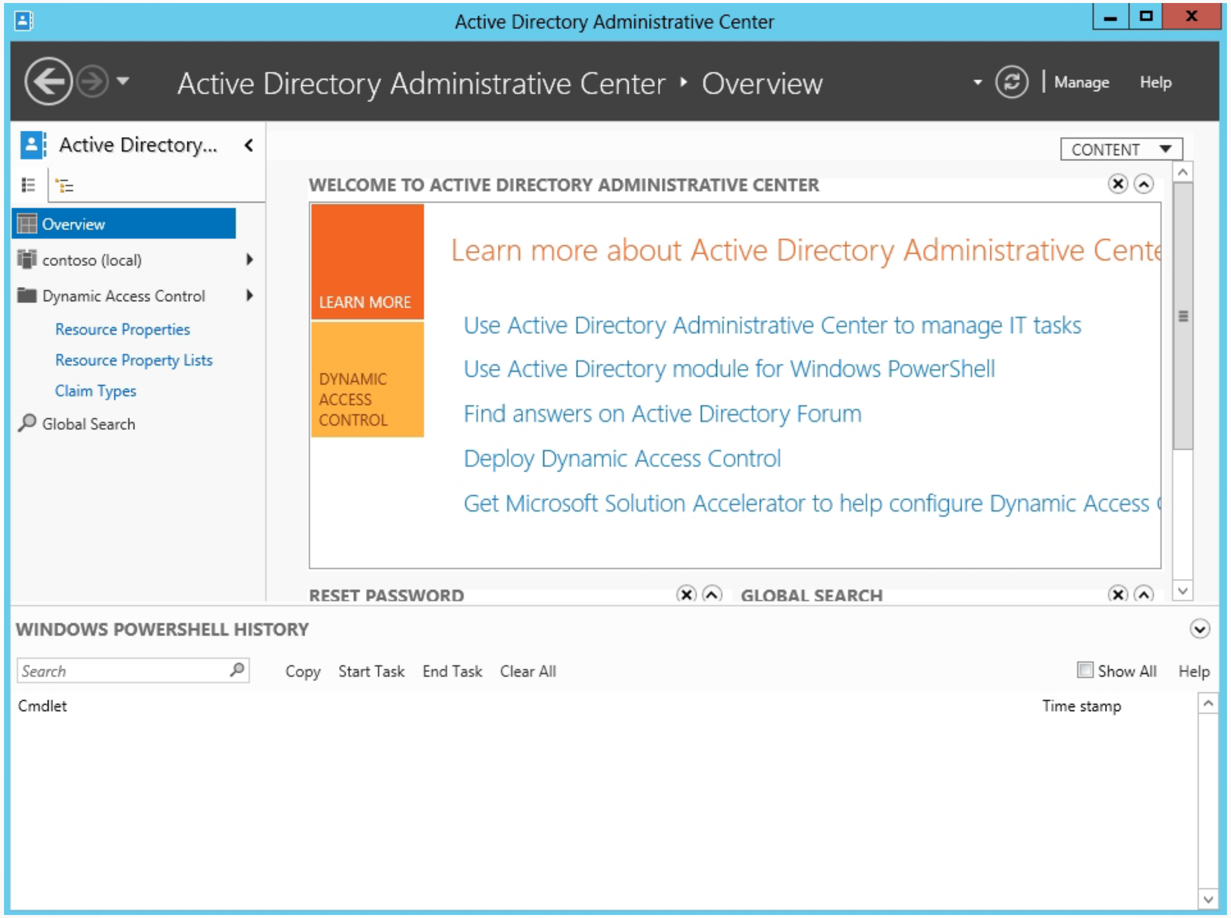
Enabling the Recycle Bin

In Windows Server 2012, you can enable the Recycle Bin in two ways:

- From the Active Directory module for Windows PowerShell prompt, use the `Enable-ADOptionalFeature` cmdlet.
- From Active Directory Administrative Center, select the domain, and then click *Enable Active Directory Recycle Bin* in the Tasks pane.

Only items deleted after the Active Directory Recycle Bin is turned on can be restored from the Active Directory Recycle Bin.

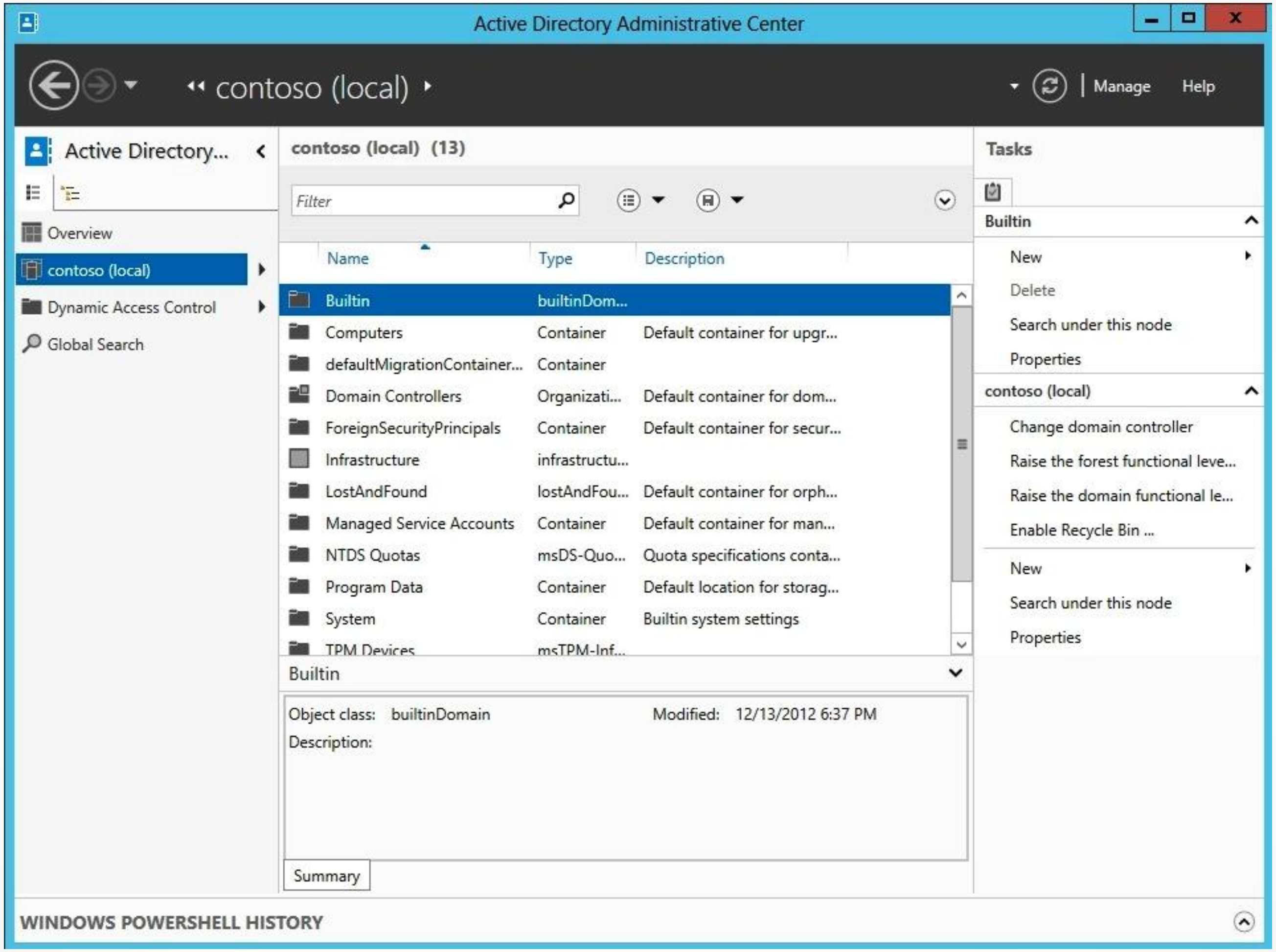
Enable the Active Directory Recycle Bin



Active Directory Administrative Center
Active Directory Administrative Center ‣ Overview
Manage
Help
Active Directory...
Overview
contoso (local)
Dynamic Access Control
Resource Properties
Resource Property Lists
Claim Types
Global Search
CONTENT
WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER
LEARN MORE
DYNAMIC ACCESS CONTROL
Learn more about Active Directory Administrative Cente
Use Active Directory Administrative Center to manage IT tasks
Use Active Directory module for Windows PowerShell
Find answers on Active Directory Forum
Deploy Dynamic Access Control
Get Microsoft Solution Accelerator to help configure Dynamic Access
RESET PASSWORD
GLOBAL SEARCH
WINDOWS POWERSHELL HISTORY
Search
Copy
Start Task
End Task
Clear All
□ Show All
Help
Cmdlet
Time stamp

Opening Active Directory Administrative Center

Enable the Active Directory Recycle Bin



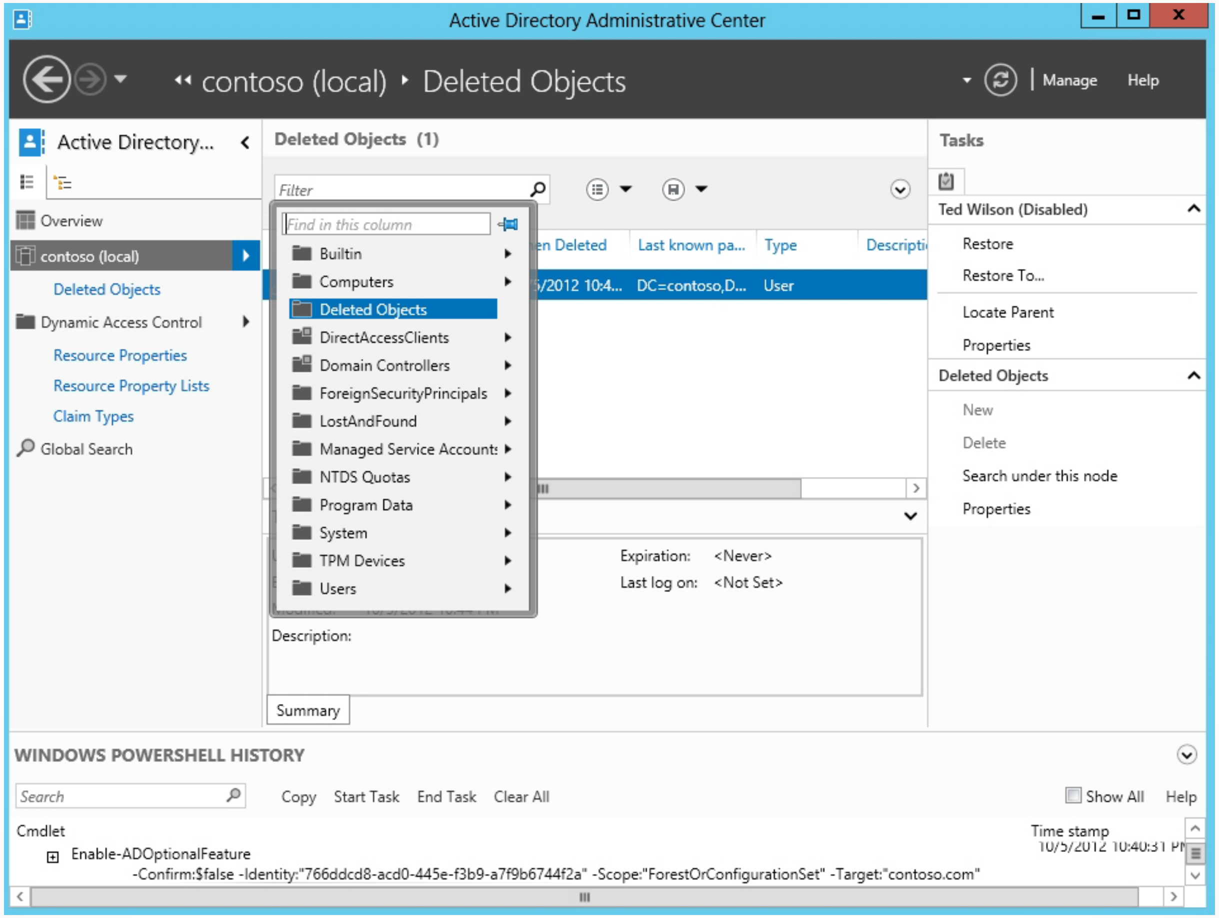
Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
defaultMigrationContainer...	Container	
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	

Builtin

Object class: builtinDomain   Modified: 12/13/2012 6:37 PM
Description:

Selecting the domain options

Restore an Object Using the Active Directory Recycle Bin



/5/2012 10:4... DC=contoso,D... User

Expiration: <Never>

Last log on: <Not Set>

Description:

```
Enable-ADOptionalFeature
    -Confirm:$false -Identity:"766ddcd8-acd0-445e-f3b9-a7f9b6744f2a" -Scope:"ForestOrConfigurationSet" -Target:"contoso.com"
```

10/5/2012 10:40:31 PM

Selecting the Deleted Objects folder

Managing Active Directory Offline

Lesson 17: Maintaining Active Directory

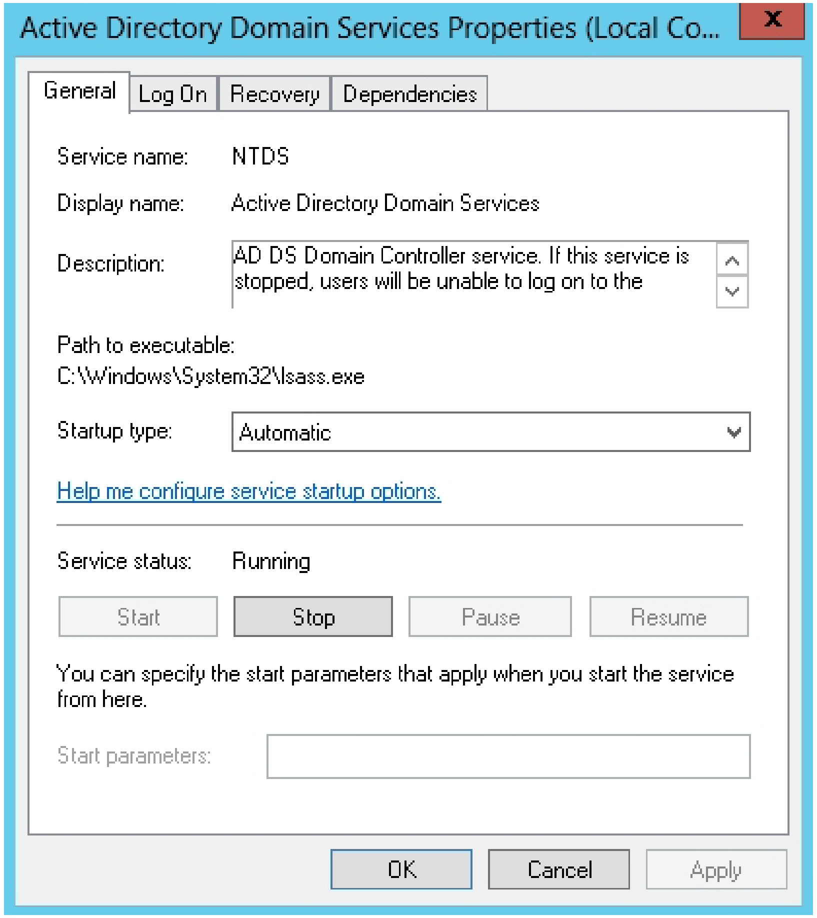
Restartable Active Directory Domain Services

Starting with Windows Server 2012, Windows servers include ***Restartable Active Directory Domain Services***, which allows you to stop and start AD DS without restarting the domain controller and stopping other services that might be on the server.

To start or stop the AD DS, open the Services console to control the service. There are three domain controller states:

- AD DS Started
- AD DS Stopped
- DSRM

Working with the Deleted Objects Folder



Service name: NTDS

Display name: Active Directory Domain Services

Description: AD DS Domain Controller service. If this service is stopped, users will be unable to log on to the

Path to executable:
C:\Windows\System32\lsass.exe

Startup type: Automatic

Help me configure service startup options.

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Selecting the Deleted Objects folder

Optimizing an Active Directory Database

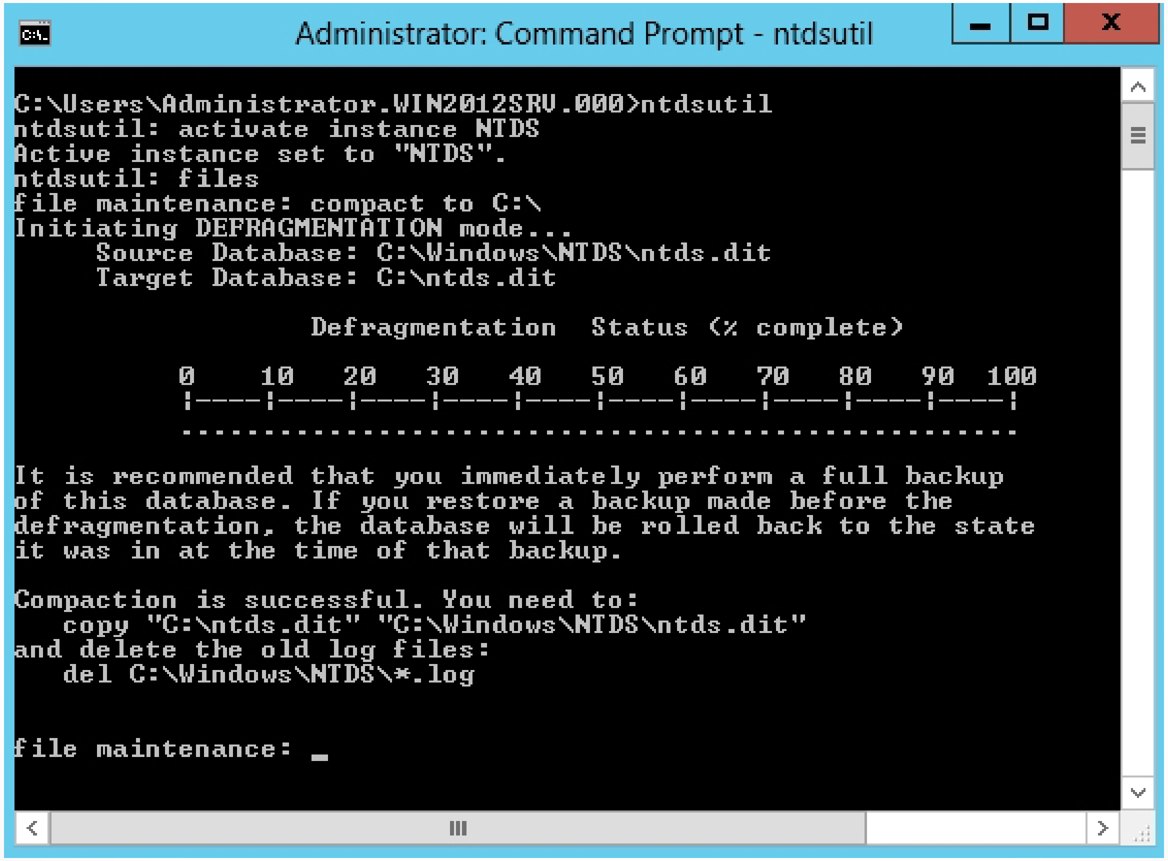
Lesson 17: Maintaining Active Directory

Ntdsutil.exe

The `ntdsutil` tool:

- Defragments the Active Directory database to free up disk space.
- Lets you look for errors in Active Directory.
- Is similar to running the Optimize and defragment drive tool in Windows.

Defragment and Check the Integrity of the Active Directory Database



```
C:\Users\Administrator.WIN2012SRV.000>ntdsutil
ntdsutil: activate instance NTDS
Active instance set to "NTDS".
ntdsutil: files
file maintenance: compact to C:\
Initiating DEFRAGMENTATION mode...
     Source Database: C:\Windows\NTDS\ntds.dit
     Target Database: C:\ntds.dit

                  Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
   copy "C:\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
   del C:\Windows\NTDS\*.log


file maintenance: _
```

Defragmenting an Active Directory database

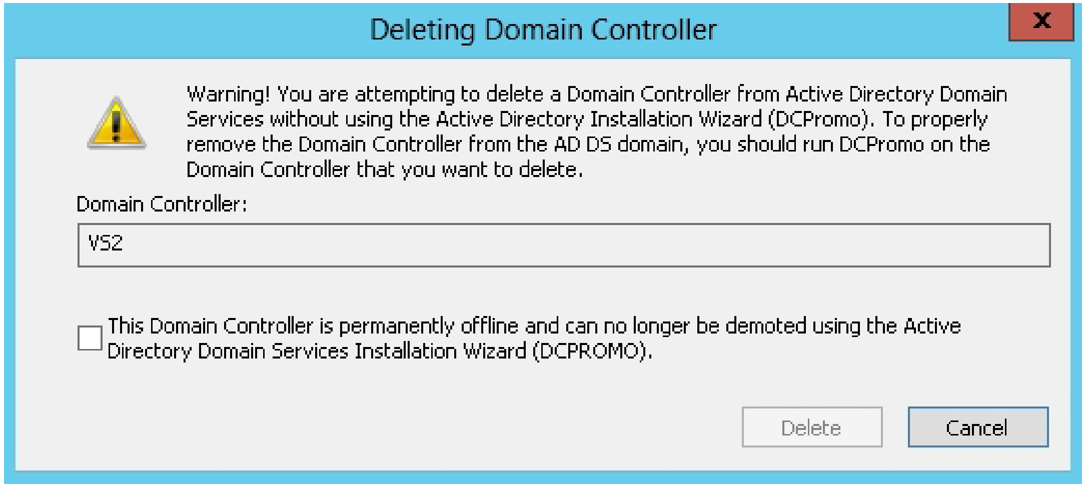
Cleaning Up Metadata

Lesson 17: Maintaining Active Directory

Metadata

- To retire a domain controller, the proper method to demote a domain controller is to remove the Active Directory Domain Services.
- If the demotion fails or the server itself fails where you cannot recover the system, you need to clean up the metadata, which means you must manually remove the domain controller from Active Directory.
- ***Metadata*** is the data that identifies the domain controllers.
- Methods for cleaning up server metadata:
  - Use Active Directory Users and Computers and `ntdsutil`.
  - Use the Active Directory Sites and Services and ADSIEdit.

Clean Up Server Metadata Using Active Directory Users and Computers



Warning! You are attempting to delete a Domain Controller from Active Directory Domain Services without using the Active Directory Installation Wizard (DCPromo). To properly remove the Domain Controller from the AD DS domain, you should run DCPromo on the Domain Controller that you want to delete.

Domain Controller: VS2

□ This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO).

Deleting the domain controller

Lesson Summary

- The CSVDE.exe and LDIFDE.exe tools enable importing to and exporting from Active Directory.
- Backing up refers to making copies of data.
- The Active Directory database is stored in an Active Directory database file (C:\Windows\NTDS\Ntds.dit) and its associated log and temporary files.
- The Windows system state is a collection of system components that are not contained in a simple file but can be backed up easily.
- The SYSVOL is a shared directory that stores the server copy of the domain’s public files that must be shared for common access and replication throughout a domain.
- Windows includes Microsoft Windows Backup, which allows you to back up a system. However, third-party backup software packages usually offer more features and options.

Lesson Summary

- With a nonauthoritative restore, you restore a backup of Active Directory as of the date of the backup.
- An authoritative restore is an override type restore that the information on the restored domain controller will be replicated to the other domain controllers.
- An Active Directory snapshot is a shadow copy, created by the Volume Shadow Copy Service (VSS), of the volumes that contain the Active Directory database and log files.
- The Active Directory Recycle Bin can be used to undelete deleted Active Directory containers and objects.
- You can use `ntdsutil` to defragment the Active Directory database to free up disk space.
- The metadata is the data that identifies the domain controllers.