Microsoft® Official Course

Module 3
Managing Active Directory Domain Services Objects
Module Overview

- Managing User Accounts
- Managing Groups
- Managing Computer Accounts
- Delegating Administration
Lesson 1: Managing User Accounts

• AD DS Administration Tools
• Creating User Accounts
• Configuring User Account Attributes
• Creating User Profiles
• Demonstration: Managing User Accounts
• Demonstration: Using Templates to Manage User Accounts
To manage AD DS objects, you can use the following graphical tools:

- Active Directory Administration snap-ins
- Active Directory Administrative Center

You can also use the following command-line tools:

- Active Directory module in Windows PowerShell
- Directory Service commands
Creating User Accounts

Create User:

Account

- First name: 
- Middle initials: 
- Last name: 
- Full name: * 
- User UPN logon: @
- User SamAccount: Adatum
- Password: 
- Confirm password: 

Account expires: 
- Never
- End of 

Password options:
- User must change password at next log on
- Other password options
  - Smart card is required for interactive log on
  - Password never expires
  - User cannot change password

Encryption options: 
- Other options:

Organization

- Display name: 
- Office: 
- E-mail: 
- Web page: 

More Information

OK Cancel
Configuring User Account Attributes

Ed Meadows

**ACCOUNT**
- First name: Ed
- Last name: Meadows
- Full name: Ed Meadows
- User UPN logon: Ed
- User SamAccountName: Adatum.com
- Account expires: Never
- Password options:
  - User must change password at next log on
  - End of
- Encryption options:
  - Store password using reversible encryption
  - Use Kerberos DES encryption types for this account

**Log on hours**
- Logon permitted: Sunday through Saturday from 12:00 AM to 12:00 AM

**Organization**
- Display name:
- Office:
- E-mail:
- Web page:
- Phone numbers: Main:

**Extensions**

**More Information**
Demonstration: Managing User Accounts

In this demonstration, you will see how to:
- Use the Active Directory Administrative Center to manage user accounts
  - Delete a user account
  - Create a new user account
  - Move the user account
- Use Windows PowerShell to manage user accounts
  - Find inactive user accounts
  - Find disabled user accounts
  - Delete disabled user accounts
Demonstration: Using Templates to Manage User Accounts

In this demonstration, you will see how to:

- Create a user template account
- Use Windows PowerShell to create a user from the user template
- Verify the properties of the new user account
Lesson 2: Managing Groups

- Group Types
- Group Scopes
- Implementing Group Management
- Default Groups
- Special Identities
- Demonstration: Managing Groups
Group Types

• Distribution groups
  • Used only with email applications
  • Not security-enabled (no SID); cannot be given permissions

• Security groups
  • Security principal with an SID; can be given permissions
  • Can also be email-enabled

Both security groups and distribution groups can be converted to the other type of group.
# Group Scopes

<table>
<thead>
<tr>
<th>Group scope</th>
<th>Members from same domain</th>
<th>Members from domain in same forest</th>
<th>Members from trusted external domain</th>
<th>Can be assigned permissions to resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local</strong></td>
<td>U, C, GG, DLG, UG and local users</td>
<td>U, C, GG, UG</td>
<td>U, C, GG</td>
<td>On the local computer only</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>U, C, GG, DLG, UG</td>
<td>U, C, GG, UG</td>
<td>U, C, GG</td>
<td>Anywhere in the domain</td>
</tr>
<tr>
<td><strong>Universal</strong></td>
<td>U, C, GG, UG</td>
<td>U, C, GG, UG</td>
<td>N/A</td>
<td>Anywhere in the forest</td>
</tr>
<tr>
<td><strong>Global</strong></td>
<td>U, C, GG</td>
<td>N/A</td>
<td>N/A</td>
<td>Anywhere in the domain or a trusted domain</td>
</tr>
</tbody>
</table>

- **U**: User
- **C**: Computer
- **GG**: Global Group
- **DLG**: Domain Local Group
- **UG**: Universal Group
Implementing Group Management

1. Identities
   Users or computers, which are members of

2. Global groups
   Which collect members based on members’ roles, which are members of

3. Domain local groups
   Which provide management such as resource access, which are

4. Assigned access to a resource

   This best practice for nesting groups is known as IGDLA.
Implementing Group Management

- Identities
  Users or computers, which are members of
Implementing Group Management

I Identities
Users or computers, which are members of

G Global groups
Which collect members based on members’ roles, which are members of
Implementing Group Management

1. Identities
   Users or computers, which are members of

2. Global groups
   Which collect members based on members’ roles, which are members of

3. Domain local groups
   Which provide management such as resource access, which are
Implementing Group Management

1. Identities
   Users or computers, which are members of

2. Global groups
   Which collect members based on members’ roles, which are members of

3. Domain local groups
   Which provide management such as resource access, which are

4. Assigned access to a resource
Implementing Group Management

1. Identities
   Users or computers, which are members of

2. Global groups
   Which collect members based on members’ roles, which are members of

3. Domain local groups
   Which provide management such as resource access, which are

4. Assigned access to a resource

This best practice for nesting groups is known as IGDLA.
**Default Groups**

- Carefully manage the default groups that provide administrative privileges, because these groups:
  - Typically have broader privileges than are necessary for most delegated environments
  - Often apply protection to their members

<table>
<thead>
<tr>
<th>Group</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Admins</td>
<td>Users container of the forest root domain</td>
</tr>
<tr>
<td>Schema Admins</td>
<td>Users container of the forest root domain</td>
</tr>
<tr>
<td>Administrators</td>
<td>Built-in container of each domain</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Users container of each domain</td>
</tr>
<tr>
<td>Server Operators</td>
<td>Built-in container of each domain</td>
</tr>
<tr>
<td>Account Operators</td>
<td>Built-in container of each domain</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Built-in container of each domain</td>
</tr>
<tr>
<td>Print Operators</td>
<td>Built-in container of each domain</td>
</tr>
<tr>
<td>Cert Publishers</td>
<td>Users container of each domain</td>
</tr>
</tbody>
</table>
• Special identities:
  • Are groups for which membership is controlled by the operating system
  • Can be used by the Windows Server operating system to provide access to resources:
    • Based on the type of authentication or connection
    • Not based on the user account

• Important special identities include:
  • Anonymous Logon
  • Authenticated Users
  • Everyone
  • Interactive
  • Network
  • Creator Owner
In this demonstration, you will see how to:

- Create a new group
- Add members to the group
- Add a user to the group
- Change the group type and scope
- Modifying the group’s Managed By property
Lesson 3: Managing Computer Accounts

- What Is the Computers Container?
- Specifying the Location of Computer Accounts
- Controlling Permissions to Create Computer Accounts
- Performing an Offline Domain Join
- Computer Accounts and Secure Channels
- Resetting the Secure Channel
- Bring Your Own Device
What Is the Computers Container?
Specifying the Location of Computer Accounts

- Best practice is to create Organizational Units (OUs) for computer objects
  - Servers
    - Typically subdivided by server role
  - Client computers
    - Typically subdivided by region

- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy
Controlling Permissions to Create Computer Accounts

Active Directory Users and Computers

Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:
- This folder, existing objects in this folder, and creation of new objects in this folder
- Only the following objects in the folder:
  - account objects
  - aCSResourceLimits objects
  - applicationVersion objects
  - bootableDevice objects
  - certificationAuthority objects
  - Computer objects
- Create selected objects in this folder
- Delete selected objects in this folder

< Back  Next >  Cancel  Help
Performing an Offline Domain Join

Offline Domain join can is used to join computers to a Domain when they cannot contact a domain controller.

- Create a domain join file using:
  ```
djoin.exe /requestODJ /LoadFile <filepath>
/WindowsPath <path to the Windows directory of the offline image>
  ```

- Import the domain join file using:
  ```
djoin.exe /requestODJ /LoadFile <filepath>
/WindowsPath <path to the Windows directory of the offline image>
  ```
Computer Accounts and Secure Channels

• Computers have accounts
  • sAMAccountName and password
  • Used to create a secure channel between the computer and a domain controller
• Scenarios where a secure channel can be broken
  • Reinstalling a computer, even with same name, generates a new SID and password
  • Restoring a computer from an old backup, or rolling back a computer to an old snapshot
  • Computer and domain disagree about what the password is
Resetting the Secure Channel

• Do not delete a computer from the domain and rejoin
  • This process creates a new account, resulting in new SID and lost group memberships

• Options for resetting the secure channel
  • Active Directory Users and Computers
  • DSMod.exe
  • NetDom.exe
  • NLTest.exe
  • Windows PowerShell
Bring Your Own Device

AD FS has been enhanced to support bring your own device programs

• Workplace Join – Creates an AD DS object for consumer devices
• Multi-Factor Access Control – Increases security by using claims-based authorization rules
• Multi-Factor Authentication – Increases security by requiring more than one form of authentication
• Web Application Proxy – Allows apps to be securely publish to the Internet
Lesson 4: Delegating Administration

- Considerations for Using Organizational Units
- AD DS Permissions
- Effective AD DS Permissions
- Demonstration: Delegating Administrative Permissions
Considerations for Using Organizational Units

- OUs allow you to subdivide the Domain for management purposes
- OUs are used for:
  - Delegation of control
  - Application of GPOs
- The OU structure can be:
  - Flat, one to two levels deep
  - Deep, more than 5 levels deep
  - Narrow, anything in between
AD DS Permissions

Active Directory Users and Computers

Advanced Security Settings for IT

Owner: Domain Admins (ADATUM\Domain Admins) Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADATUM)</td>
<td>Create/delete InetOrgRoot</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADATUM)</td>
<td>Create/delete Computer</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADATUM)</td>
<td>Create/delete Group</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADATUM\Print)</td>
<td>Create/delete Printer</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADATUM)</td>
<td>Create/delete User obj</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADATUM\Domain Admin)</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLER</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
</tbody>
</table>

Add Remove View

Disable inheritance

Restore defaults

OK Cancel Apply
Effective AD DS Permissions

Permissions assigned to users and groups accumulate

Best practice is to assign permissions to groups, not to individual users

In the event of conflicts:
  • Deny permissions override Allow permissions
  • Explicit permissions override Inherited permissions
    • Explicit Allow overrides Inherited Deny

To evaluate effective permissions, you can use:
  • The Effective Access tab
  • Manual analysis
Demonstration: Delegating Administrative Permissions

In this demonstration, you will see how to:

• Create an OU
• Move objects into an OU
• Delegate a standard task
• Delegate a custom task
• View AD DS permissions resulting from these delegations
Lab: Managing Active Directory Domain Services Objects

• Exercise 1: Delegating Administration for a Branch Office
• Exercise 2: Creating and Configuring User Accounts in AD DS
• Exercise 3: Managing Computer Objects in AD DS

**Logon Information**

Virtual machines 20410C-LON-DC1

20410C-LON-CL1

User name  Adatum\Administrator

Password  Pa$$w0rd

Estimated Time: 60 minutes
Lab Scenario

You have been working for A. Datum as a desktop support specialist and have visited desktop computers to troubleshoot app and network problems. You have recently accepted a promotion to the server support team. One of your first assignments is configuring the infrastructure service for a new branch office.

(Continued on next slide)
To begin deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create an OU for the branch office and delegate permission to manage it. Then you need to create users and groups for the new branch office. Finally, you need to reset the secure channel for a computer account that has lost connectivity to the domain in the branch office.
Lab Review

• What are the options for modifying the attributes of new and existing users?
• What types of objects can be members of global groups?
• What types of objects can be members of domain local groups?
• What are the two credentials that are necessary for any computer to join a domain?
Module Review and Takeaways

• Review Questions
• Best Practices
• Tools