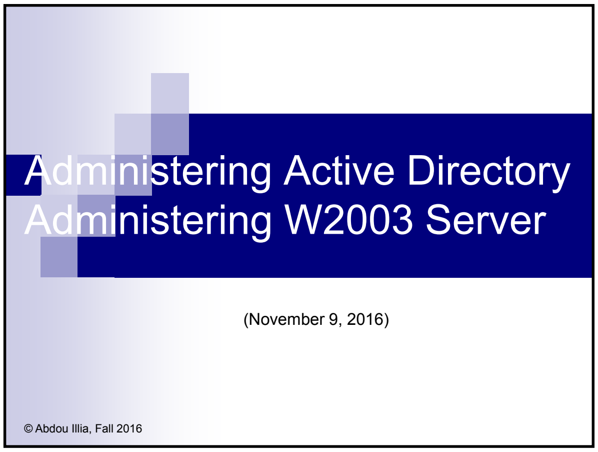
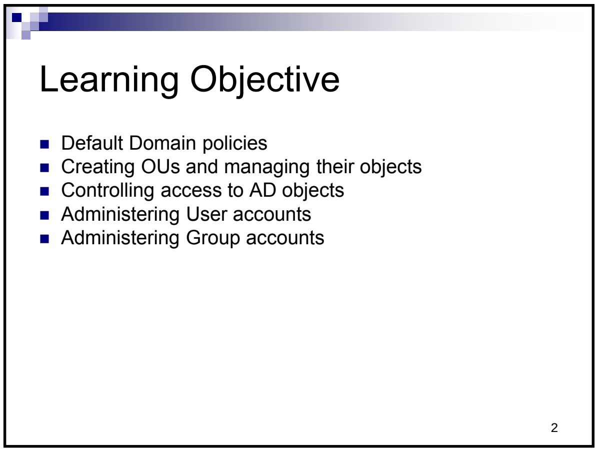


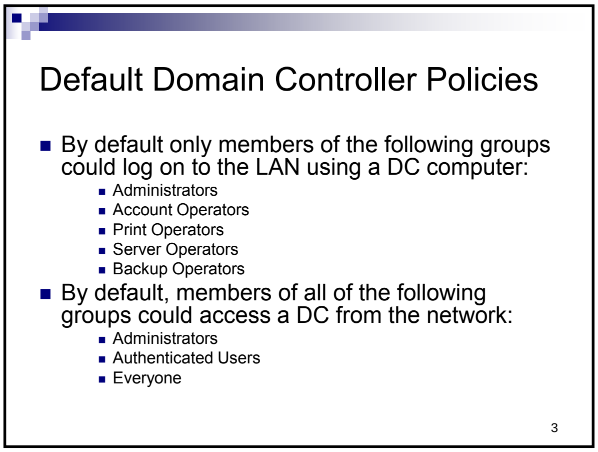
Administering Active Directory Administering W2003 Server

(November 9, 2016)



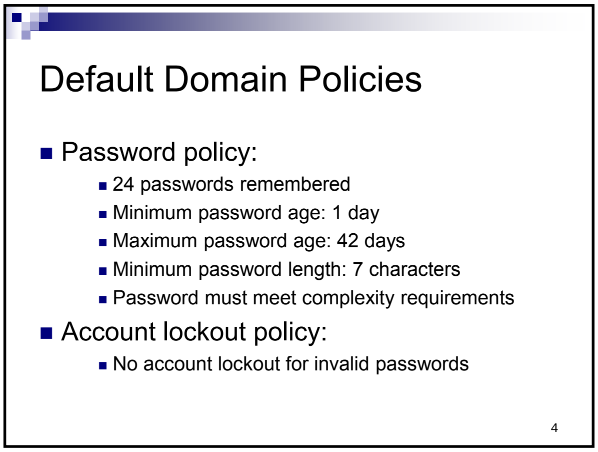
Learning Objective

- Default Domain policies
- Creating OUs and managing their objects
- Controlling access to AD objects
- Administering User accounts
- Administering Group accounts



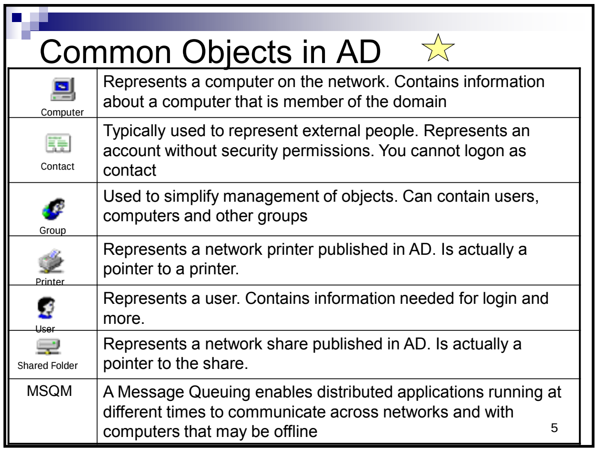
Default Domain Controller Policies

- By default only members of the following groups could log on to the LAN using a DC computer:
  - Administrators
  - Account Operators
  - Print Operators
  - Server Operators
  - Backup Operators
- By default, members of all of the following groups could access a DC from the network:
  - Administrators
  - Authenticated Users
  - Everyone



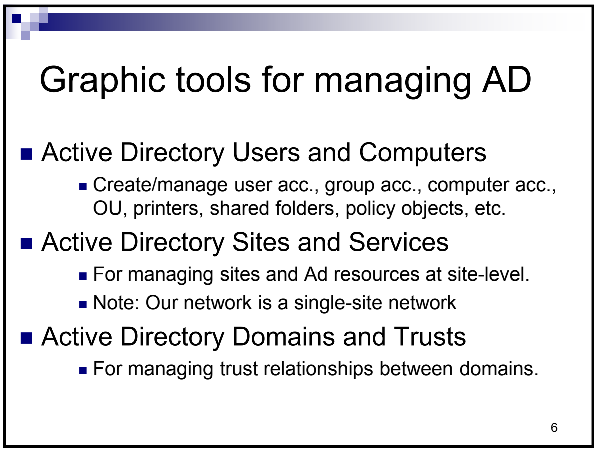
Default Domain Policies

- Password policy:
  - 24 passwords remembered
  - Minimum password age: 1 day
  - Maximum password age: 42 days
  - Minimum password length: 7 characters
  - Password must meet complexity requirements
- Account lockout policy:
  - No account lockout for invalid passwords



Common Objects in AD ☆

Computer	Represents a computer on the network. Contains information about a computer that is member of the domain
Contact	Typically used to represent external people. Represents an account without security permissions. You cannot logon as contact
Group	Used to simplify management of objects. Can contain users, computers and other groups
Printer	Represents a network printer published in AD. Is actually a pointer to a printer.
User	Represents a user. Contains information needed for login and more.
Shared Folder	Represents a network share published in AD. Is actually a pointer to the share.
MSQM	A Message Queuing enables distributed applications running at different times to communicate across networks and with computers that may be offline



Graphic tools for managing AD

- Active Directory Users and Computers
  - Create/manage user acc., group acc., computer acc., OU, printers, shared folders, policy objects, etc.
- Active Directory Sites and Services
  - For managing sites and Ad resources at site-level.
  - Note: Our network is a single-site network
- Active Directory Domains and Trusts
  - For managing trust relationships between domains.

Command-line tools for managing AD

- **dsadd** for adding objects such as:
  - user acc., group acc., OUs, etc.
- **dsmod** for modifying objects attributes
- **dsmove** for moving objects within AD
- **dsrm** for removing objects from AD

Dsadd user command-line

- Syntax:

```
dsadd user UserDN [-samid SAMName] [-upn UPN] [-fn FirstName] [-mi
Initial] [-ln LastName] [-display DisplayName] [-empid EmployeeID] [-pwd
{Password | *}] [-desc Description] [-memberof Group;...] [-office Office] [-tel
PhoneNumber] [-email Email] [-hometel HomePhoneNumber] [-pager
PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel
IPPhoneNumber] [-webpg WebPage] [-title Title] [-dept Department] [-
company Company] [-mgr Manager] [-hmdir HomeDirectory] [-hmdrv
DriveLetter:] [-profile ProfilePath] [-loscr ScriptPath] [-mustchpwd {yes | no}]
[-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes |
no}] [-acctexpires NumberOfDays] [-disabled {yes | no}] [{-s Server | -d
Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]
```

- UserDN specifies the **distinguished name** of the user
- SAMName specifies the SAM account name (e.g. jdoe)
- *UPN* specifies the user principal name (e.g. jdoe@newcontoso.com)
- *GroupDN* specifies the distinguished names of the groups the user belongs to.

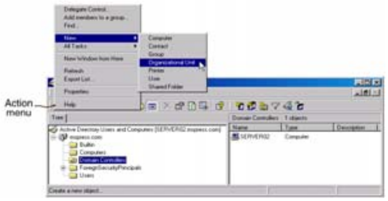
Creating OUs

- You should create an OU:
  - ▶ To group objects that require similar administrative tasks. Example: Creating an OU for all temporary employees or for Sales department.
  - ▶ To delegate administrative control to other users.
- You can create an OU under a domain, under a Domain Controller object, or within another OU
- To create an OU, you must have required permission* to add OUs in the OU, under the domain, or under the Domain Controller object.

Note: * By default, all members of the Administrators group have that permission

Creating OUs

1) Open the Active Directory Users and Computers snap-in
2) Select the domain or existing OU where you want to create the OU
3) Click the Action menu. Point to New, then click Organizational Unit.
4) Type the name of the new OU in the Name text box. Click OK



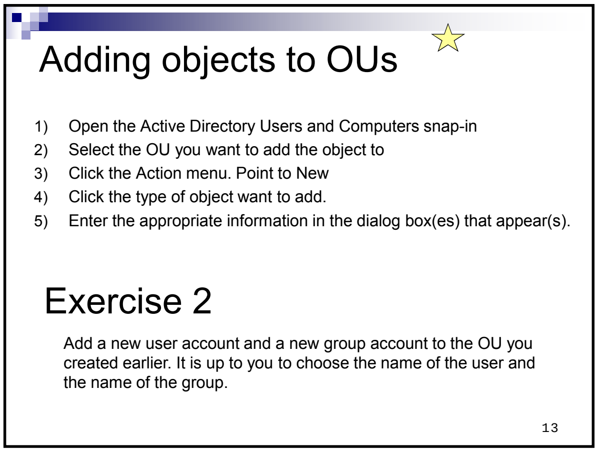
Exercise 1

- **Create a new OU named LastNameOU (where LastName is your last name). The new OU should be directly under your domain (e.g. group1.mis3200.com or team2.contoso.com)**

  Note: It may take a few minutes before the replication takes place. After replication, all users who are logged onto the domain can see the new OU.

Exercise 1 (continued)

- **Suppose that the replication takes a long time to complete. What if two OUs with the same name are created? Explain what would happen.**
- **Open the Active Directory Users and Computers snap-in. Click Action/Refresh. How many OUs do you see?**

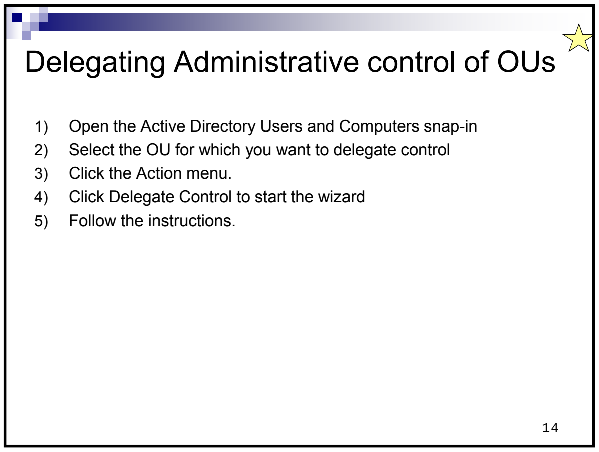


Adding objects to OUs

1) Open the Active Directory Users and Computers snap-in
2) Select the OU you want to add the object to
3) Click the Action menu. Point to New
4) Click the type of object want to add.
5) Enter the appropriate information in the dialog box(es) that appear(s).

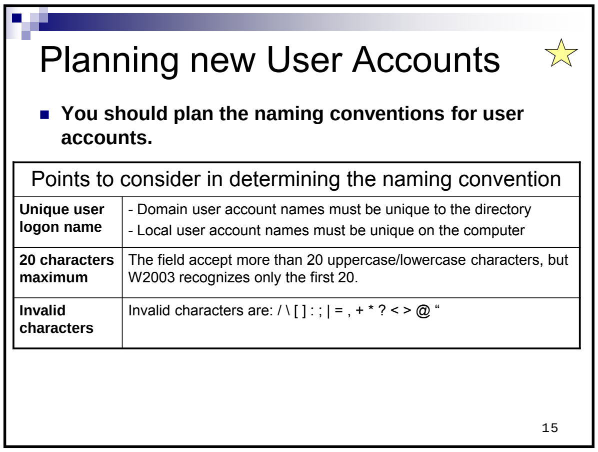
Exercise 2

Add a new user account and a new group account to the OU you created earlier. It is up to you to choose the name of the user and the name of the group.



Delegating Administrative control of OUs

1) Open the Active Directory Users and Computers snap-in
2) Select the OU for which you want to delegate control
3) Click the Action menu.
4) Click Delegate Control to start the wizard
5) Follow the instructions.



Planning new User Accounts

- **You should plan the naming conventions for user accounts.**

<table>
<tr><th colspan="2">Points to consider in determining the naming convention</th></tr>
<tr><td><b>Unique user logon name</b></td><td>- Domain user account names must be unique to the directory
- Local user account names must be unique on the computer</td></tr>
<tr><td><b>20 characters maximum</b></td><td>The field accept more than 20 uppercase/lowercase characters, but W2003 recognizes only the first 20.</td></tr>
<tr><td><b>Invalid characters</b></td><td>Invalid characters are: / \ [ ] : ; | = , + * ? < > @ “</td></tr>
</table>

Planning new User Accounts

- **You should, also, plan Account options, such as logon hours, computers from which users can logon, and account expiration.**

Logon hours	By default W2003 allows users to access 24/7. You can determine the logon days/hours.
Computers from which users can logon	By default, users can logon to the domain by using any computer in the domain. For security, you can restrict users to logging on only from their own computers.

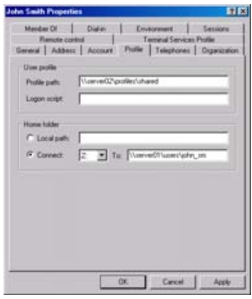
Administering user accounts

- **Use the Active Directory Users and Computers snap-in to create Domain user accounts**

Common Administrative tasks	
Disabling and Enabling User Accounts	Account can be disabled for security reasons.
Lock/Unlocking User Accounts	Account can be locked when the user violates a Group policy.
Resetting Passwords	No need to know the user password. Right-click the appropriate user account, and click Reset Password
Moving User Accounts in a domain	You can move an account from one OU to another. Object permissions assigned directly to the user account move with the user account. Permissions inherited from parent object no longer apply.

Administering user accounts: User Profiles

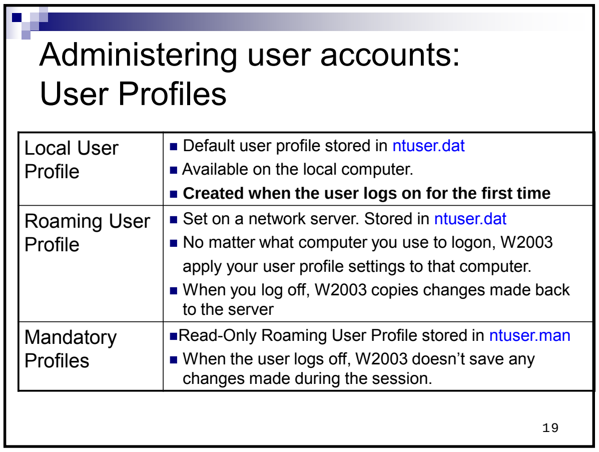
- A user profile is a collection of folders and data that stores your current desktop environment and application settings as well as personal data.
- Microsoft Windows 2003 creates a local user profile the first time you log on at a computer.
- By default, User profiles in the ntuser.dat file in the *Documents and Settings\username* folder



John Smith Properties

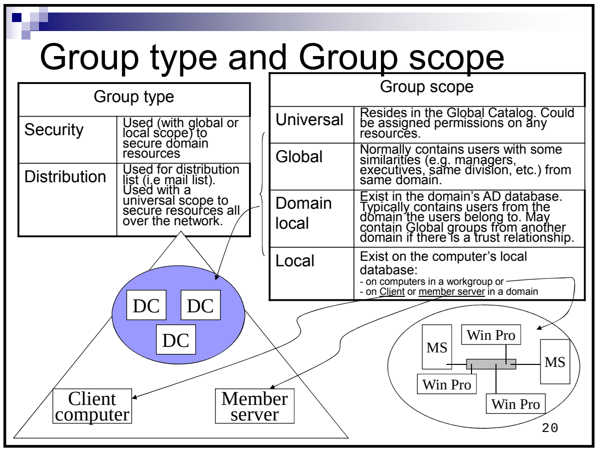
User profile
Profile path: \\server02\profiles\shared
Logon script:

Home folder
○ Local path:
● Connect: Z: To: \\server01\users\john_sm



Administering user accounts: User Profiles

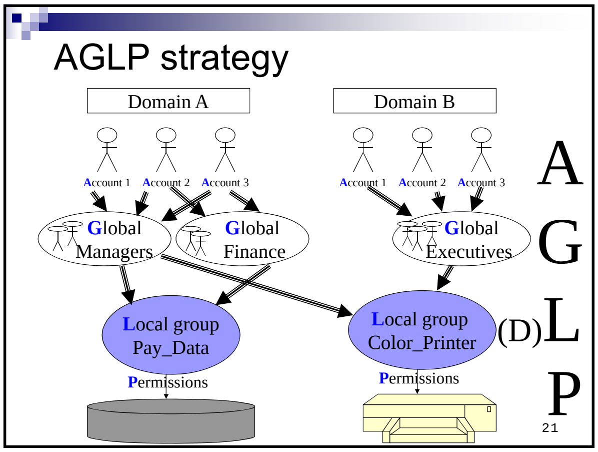
Local User Profile	■ Default user profile stored in ntuser.dat ■ Available on the local computer. ■ **Created when the user logs on for the first time**
Roaming User Profile	■ Set on a network server. Stored in ntuser.dat ■ No matter what computer you use to logon, W2003 apply your user profile settings to that computer. ■ When you log off, W2003 copies changes made back to the server
Mandatory Profiles	■Read-Only Roaming User Profile stored in ntuser.man ■ When the user logs off, W2003 doesn't save any changes made during the session.



Group type and Group scope

Group type	
Security	Used (with global or local scope) to secure domain resources
Distribution	Used for distribution list (i.e mail list). Used with a universal scope to secure resources all over the network.

Group scope	
Universal	Resides in the Global Catalog. Could be assigned permissions on any resources.
Global	Normally contains users with some similarities (e.g. managers, executives, same division, etc.) from same domain.
Domain local	Exist in the domain's AD database. Typically contains users from the domain the users belong to. May contain Global groups from another domain if there is a trust relationship.
Local	Exist on the computer's local database: - on computers in a workgroup or - on Client or member server in a domain

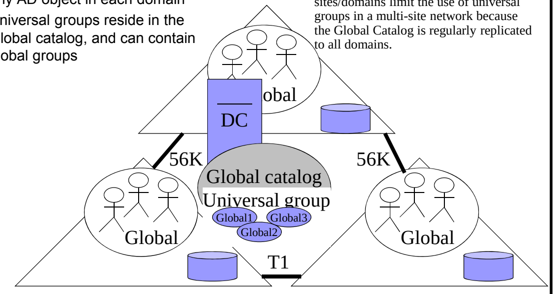


AGLP strategy

Understanding Universal groups

- Global catalog (stored on 1st DC) contains partial information about any AD object in each domain
- Universal groups reside in the Global catalog, and can contain global groups

- Universal groups could be assigned permissions on network resources
- Low speed connections between sites/domains limit the use of universal groups in a multi-site network because the Global Catalog is regularly replicated to all domains.



Note: Security Universal groups can only be created in native mode. To change mode: (1) Go to AD Users and Computers, (2) Right-click the domain, (3) Click Properties, (4) Click Change Mode

70-215:3 @ 18:00/33:00

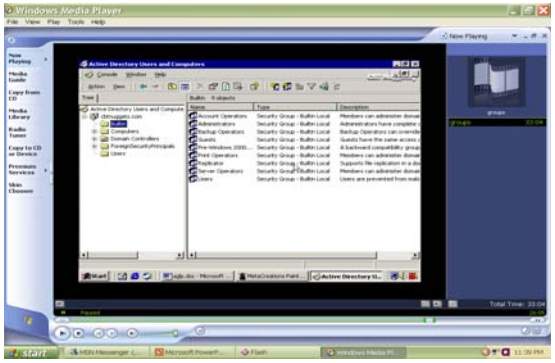
AGUP strategy

- Create user **a**ccounts in each domain as needed
- Create appropriate **g**lobal groups in each domain as needed and add individual accounts to them
- Create appropriate **u**niversal groups and add appropriate global groups to them
- Assign **p**ermissions on network resources to universal groups.

A
G
U
P

Note: Microsoft suggests using an AGULP strategy

Built-in Groups

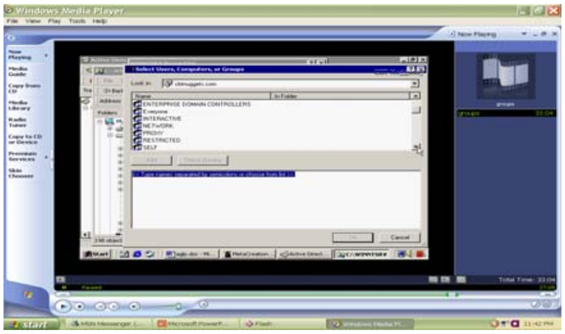


Builtin 9 objects

Name	Type	Description
Account Operators	Security Group - Builtin Local	Members can administer domai
Administrators	Security Group - Builtin Local	Administrators have complete
Backup Operators	Security Group - Builtin Local	Backup Operators can overrid
Guests	Security Group - Builtin Local	Guests have the same access
Pre-Windows 2000...	Security Group - Builtin Local	A backward compatibility grou
Print Operators	Security Group - Builtin Local	Members can administer domai
Replicator	Security Group - Builtin Local	Supports file replication in a do
Server Operators	Security Group - Builtin Local	Members can administer domai
Users	Security Group - Builtin Local	Users are prevented from mak

Special groups

- Can be seen in Security tab when assigning permissions
- Automatically generated. You cannot change their membership.



ENTERPRISE DOMAIN CONTROLLERS
Everyone
INTERACTIVE
NETWORK
PROXY
RESTRICTED
SELF