

# Account Management

## Lesson 6

# Agenda

- ❖ Explain how to **manage user accounts**
- ❖ Work with **user profiles**
- ❖ Describe factors in managing **group accounts**
- ❖ Work with **computer accounts**
- ❖ Describe tools for **automating account management**

# User Accounts



## ❖ Local User Accounts

- The **local administrator** gets total control over what accounts are created, and **only accounts created on that system can be used to log on** to that system
  - The details of these accounts are stored in the **Security Accounts Manager (SAM)** DB of the local computer

## ❖ Domain User Accounts

- Created by **domain administrator** in AD
- Can usually **log on to any computers in the AD forest**
- Stored in AD DB and replicated to all **Domain Controllers**

## ❖ Built-in User Accounts: **Administrator, Guest**

- Reside in SAM DB (*local built-in accounts*)
- Reside in AD DB (*domain built-in accounts*)

# Managing User Accounts

- ❖ The following guidelines apply to the built-in Administrator account:
  - **Local administrator** account has full access to all aspects of a **computer**, while **domain administrator** account has full access to all aspects of the **domain**
  - Administrator account should **only be used while performing administrative operations**
  - Administrator account **can be renamed or disabled but not deleted**
  - Default “Administrator” account should be renamed and given a **strong password**

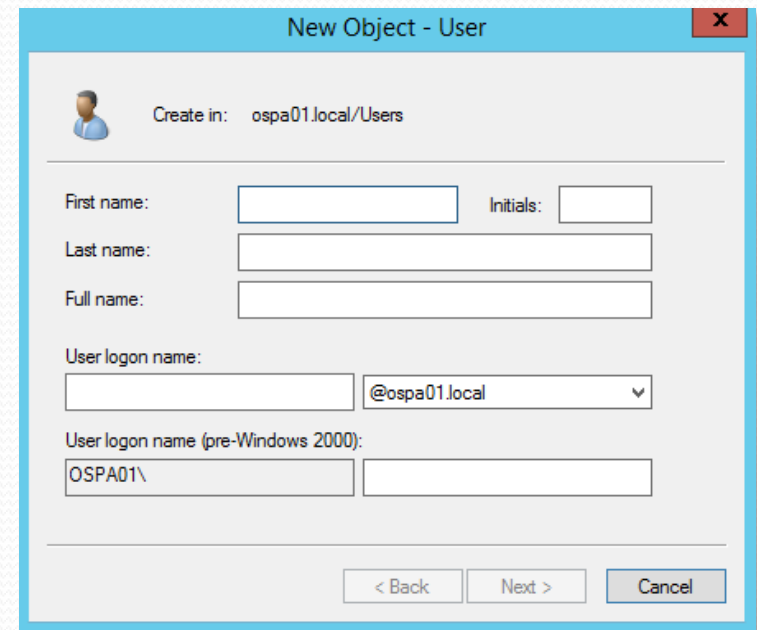
# Managing User Accounts (cont.)

- ❖ The following guidelines apply to the built-in **Guest** account:
  - **Disabled by default** and must be enabled before it can be used for logon
  - **Can have a blank password**
  - Should be renamed if it is to be used
  - Has limited access to a computer or domain  
BUT has **access to any resources for which the “Everyone” group has permission**

# Creating User Accounts

## ❖ Naming Conventions:

- Logon name and Full name must be **unique**
- Names are **case insensitive**
- Logon name can be in any number of characters
  - BUT better to be use **1-20 characters** (*limitation of the pre-Windows 2000 logon name*)
  - Can include a combination of special alphanumeric characters
- Passwords are **case sensitive**
  - By default, **complex passwords** are required



New Object - User

Create in: ospa01.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:  @ospa01.local

User logon name (pre-Windows 2000): OSPA01\

< Back Next > Cancel

# Creating User Accounts (cont.)

## ❖ Creating and modifying user accounts:

- Develop a standard naming convention (e.g.: *Don Ho* → *d.ho*)
  - Accommodates duplicate user names
  - Identifies temporary users
- Defaults only require a logon name and password to create a valid user using command-line tools BUT additional information should be provided to facilitate AD searches
- Tools
  - **Active Directory Users and Computers** MMC Snap-in (`dsa.msc`)
  - Windows command line tools (`net user /?`)
  - Directory Service command line tools (`dsadd user /?`)
  - PowerShell cmdlets (`help New-ADUser`)

More: <http://www.isunshare.com/windows-2012/net-user-command-for-windows-server-2012-r2.html>  
<https://technet.microsoft.com/en-us/library/cc731279.aspx>

# Creating User Accounts (cont.)

❖ In using GUI (Active Directory Users and Computers MMC Snap-in), the following attributes should be entered:

- Full name
- User logon name
- User logon name (pre-Windows 2000)
- Password, Confirm Password
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

The image displays two overlapping screenshots of the 'New Object - User' dialog box from the Active Directory Users and Computers MMC Snap-in. The top screenshot shows the 'General' tab, where the 'Create in' field is set to 'ospa01.local/Users'. It includes input fields for 'First name', 'Initials', 'Last name', 'Full name', 'User logon name' (with a dropdown menu showing '@ospa01.local'), and 'User logon name (pre-Windows 2000)' (with 'OSPA01\' entered). The bottom screenshot shows the 'Password' tab, which includes 'Password' and 'Confirm password' input fields. Below these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom of the dialog are '< Back', 'Next >', and 'Cancel' buttons.



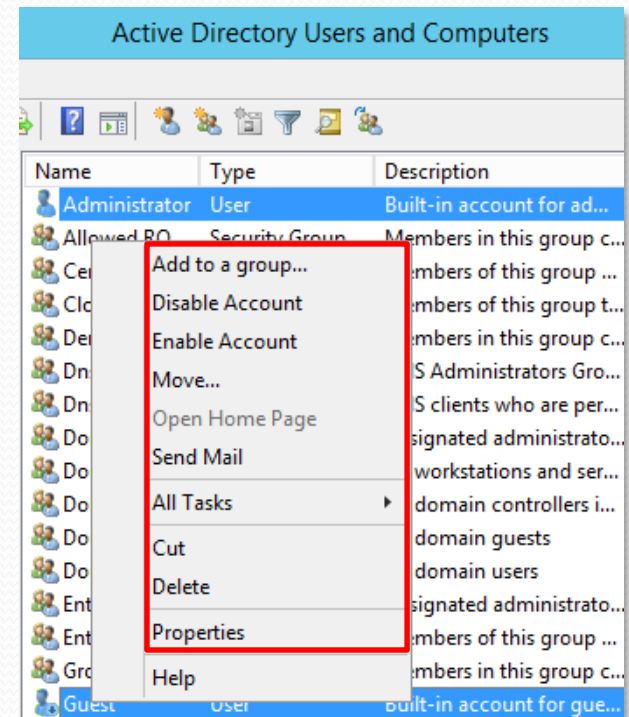
# Creating User Templates

- ❖ A **user template** is simply a **disabled normal user account**
  - that's copied to **create users with common attributes**
- ❖ Good Practice:
  - Create **ONE template account** for each department or **OU**
    - Fill in as many common attributes as you can so that less customization is necessary after the template account is created
      - **Note:** NOT all attributes can be copied!
    - **Disable** the template account to **eliminate security risks**
  - Add an underscore or other special character to the beginning of the name of the template account to make it easy to recognize
- ❖ Create a new user:
  - Right-click the user template account and then select “Copy...”
  - Modify the attributes

More: <http://www.rebeladmin.com/2014/07/create-users-with-user-templates-in-ad>

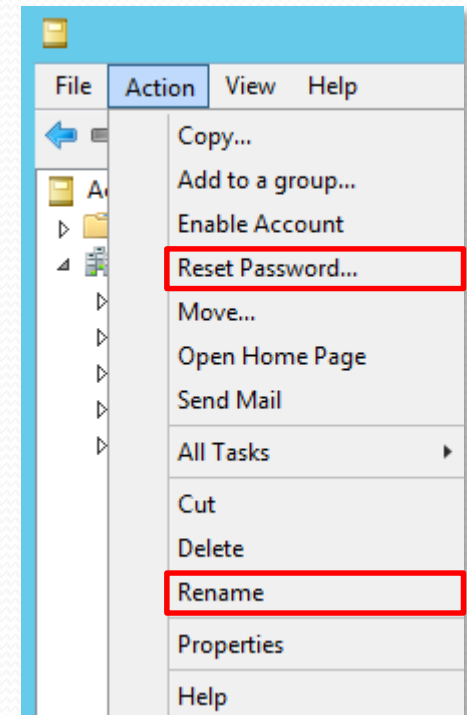
# Modifying Multiple Users

- ❖ Multiple selection in Windows can be done by:
  - <Ctrl + Click> or <Shift + Click>
- ❖ Selecting multiple users to perform the following actions simultaneously:
  - Add to a group...
  - Disable Account
  - Enable Account
  - Move... (*to another container*)
  - Send Mail
  - Cut (*and then Paste*  $\Rightarrow$  Move)
  - Delete
  - Properties



# User Account Properties

- ❖ Some account changes can be made ONLY by
  - (1) right-clicking a user account OR
  - (2) clicking Action in the menu bar
    - **Reset Password...**
    - **Rename** (*the logon name*)



# User Account Properties – General

## ❖ Contains general descriptive information about a user account

- NOT affect the user's logon, group memberships, rights, or permissions

## ❖ Fields worth mentioning

- **Display name**
  - Same as the **C**ommon **N**ame (**CN**) when account is first created
- **E-mail**
  - Can be used to send an e-mail to the user using the default mail application
- **Web page**
  - Can contain a URL and allows you to open it by right-clicking the account and then select "Open Home Page"

Don E. Ho Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+

General Address Account Profile Telephones Organization

Don E. Ho

First name: Don Initials: E

Last name: Ho

Display name: Don E. Ho

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

# User Account Properties – Account

❖ Contains the information that most affects a user's logon to the domain

- User logon name
- User logon name (pre-Windows 2000)
- Logon Hours
- Log On To...
- Unlock account
- Account options:
  - ...
  - Store password using reversible encryption
  - Smart card is required for interactive logon
  - Account is sensitive and cannot be delegated
  - ...
- Account expires

Don E. Ho Properties

Remote control	Remote Desktop Services Profile		COM+
Member Of	Dial-in	Environment	Sessions
General	Address	Account	Profile
		Telephones	Organization

User logon name:  
 @ospa01.local

User logon name (pre-Windows 2000):

☐ Unlock account

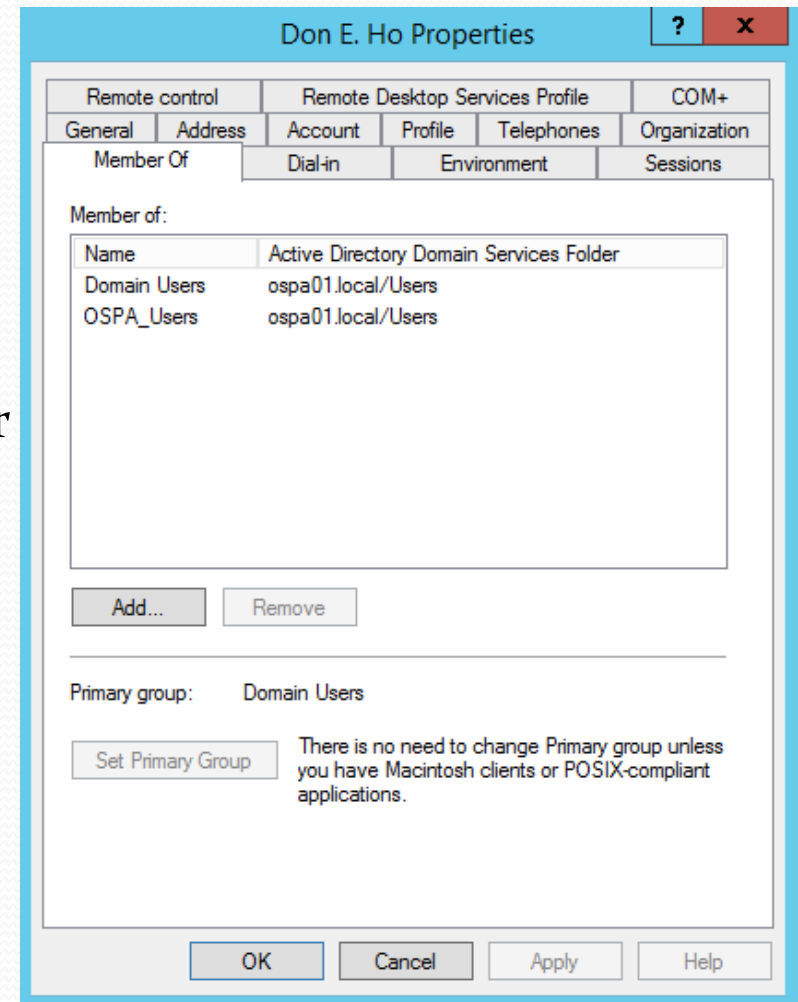
Account options:

☐ User must change password at next logon  
☐ User cannot change password  
☒ Password never expires  
☐ Store password using reversible encryption

Account expires  
☒ Never  
☐ End of:

# User Account Properties – Member Of

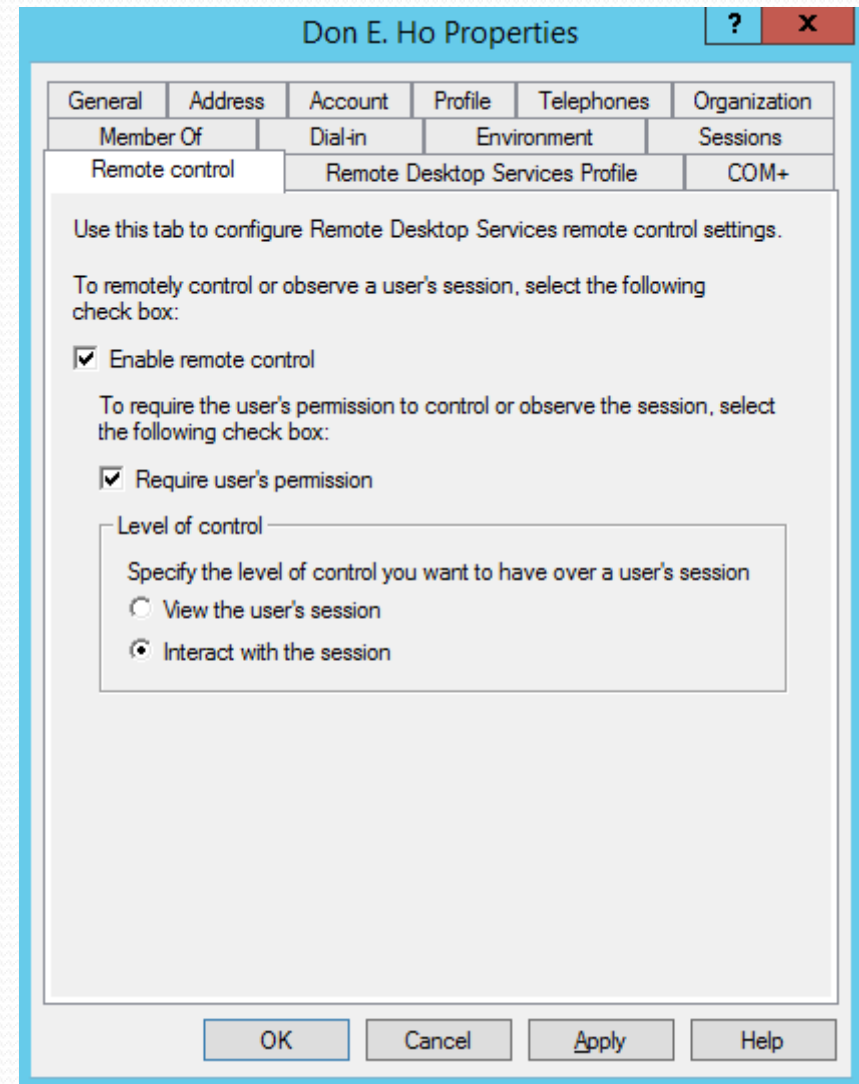
- ❖ Lists groups the user belongs to
  - Can be used to **add/remove group memberships**
  - User's **primary group** applies only to users who log on to the network through Unix, Linux or Mac computer
    - default group is **Domain Users** and no need to change in most of the cases



# User Account Properties – Remote control

❖ Remote Desktop Services (RDS), known as *Terminal Services* in Windows Server 2008 and earlier

- Allows a user to connect to a server from a remote location using port 3389





# User Account Properties – Profile

❖ Specifies the **location of files** associated with a user's characteristics and preferences

- Profile path

- Local Windows user profile is stored in `C:\Users\%username%`  
(WinXP is in `C:\Documents and Settings\`)
- User's data and settings (**roaming profile**) can be stored in a network share instead

- Logon script

- Run a script when user logs on  
(preferred to use group policy)

- Home folder

- Can be a **local path or a drive letter** that points to a network share

The screenshot shows the 'Don E. Ho Properties' dialog box with the 'Profile' tab selected. The 'User profile' section contains the following fields:

- Profile path: `%LogonServer%\Profile$\%username%`
- Logon script: `%LogonServer%\NetLOGON\login.vbs`

The 'Home folder' section has two options:

- ☐ Local path: (empty field)
- ☒ Connect: `Z:` (drive letter) To: `\\ChanTaiMan01\Home$\d.ho` (network path)

At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.



# Working with User Profiles

- ❖ A **user profile** is a collection of a user's personal files and settings that define his/her working environment
  - Establishing a user account on the computer (or on its parent domain) does not create a profile for that user
    - The **profile is created the first time** the user interactively logs on at the computer in a folder (*typically using the logon name*)
    - **Note:** Once the profile folder has been created, Windows will never automatically rename that folder even the user logon name is changed afterwards!

# Working with User Profiles (cont.)

## ❖ Key profile contents in a user's profile folder

- **AppData** (*WinXP is "Application Data"*)
- **Desktop**
- **Favorites**
- **Documents** (*WinXP is "My Documents"*)
- **Downloads** (*N/A in WinXP*)
- **Music** (*WinXP is "My Documents\My Music"*)
- **Pictures** (*WinXP is "My Documents\My Pictures"*)
- **NTuser.dat**
  - contains the **user's personalized settings** for the majority of software installed on the computer, including Windows itself
  - When the user logs on, it will **merge to the system registry** as the HKEY\_CURRENT\_USER branch
  - It is held open for writing (i.e. **locked**) whenever the user is logged on

# Working with User Profiles (cont.)

## ❖ FOUR types of profiles

### 1. Local Profile

- Is limited to the computer a user log on to and is stored on the system's local harddisk
- Is created the first time you log on to a computer by copying the settings in the **Default User profile**, and it is the default type of profile
- Any changes a user make to his/her local profile are also specific to the computer on which the user made the changes
- Default storage location
  - `%SystemDrive%\Users\%username%`
  - Old WinXP is `%SystemDrive%\Documents and Settings\%username%`

# Working with User Profiles (cont.)

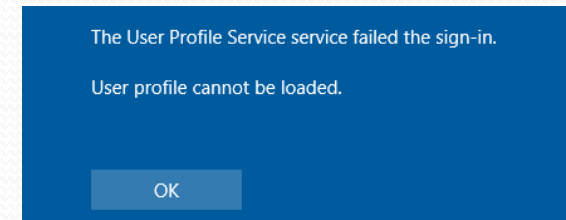
## 2. Roaming Profile

- Is stored on a network share
- Retrieved at user logon and saved as a cache copy in the local profile location of the logon computer, and transferred the locally cached copy back to the network share when the user logs off
  - ✓ A consistent profile that reflects changes made by a user on multiple networked computers
  - ✓ Simplifies user data management and allows centralized account management
  - ✗ Needs a considerable amount of time in retrieving/updating the profile
- For example, *the profile path of a domain user created in a Domain Controller:*
  - `%LogonServer%\Profile$\%username%`

# Working with User Profiles (cont.)

## 3. Mandatory (Roaming) Profile

- Is stored on a network share
- Is worked like a roaming profile BUT changes made in locally cached profile will not update the network share when the user logs off
  - Commonly used in situations where a common logon is assigned for multiple users
- Super Mandatory (Roaming) Profile
  - a mandatory user profile with an additional layer of security → prevent user from logging on if the profile is unavailable
    - With normal mandatory profile, a temporary profile will be created if it is not available when a user logs on. However, when super mandatory profile is configured, temporary profiles will not be created if it is not available over the network!



More: [http://www.linuxschools.com/karoshi/documentation/wiki/index.php?title=Creating\\_a\\_Windows\\_10\\_Mandatory\\_Profile](http://www.linuxschools.com/karoshi/documentation/wiki/index.php?title=Creating_a_Windows_10_Mandatory_Profile)

# Working with User Profiles (cont.)

## 4. Temporary Profile

- Is stored in the local profile location of the logon computer
- Is issued each time that an error condition prevents the user's profile from loading
- It will be deleted at the end of each session.



Sometimes NOT

## • Troubleshooting

- Logon as local administrator and open Event Viewer (*eventvwr.msc*)
  - Expand Windows Logs > Application
  - Look for **Source** = "User Profile Service" or **Event ID** = "1511"
- You may want to backup files in *C:\Users\TEMP...*
- Open Registry Editor (*regedit.exe*)
  - Navigate to *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList*
  - Delete those Keys having **.bak** at the end

More: <http://www.eightforums.com/tutorials/38817-youve-been-signed-temporary-profile-fix.html>

# Managing Windows Profiles

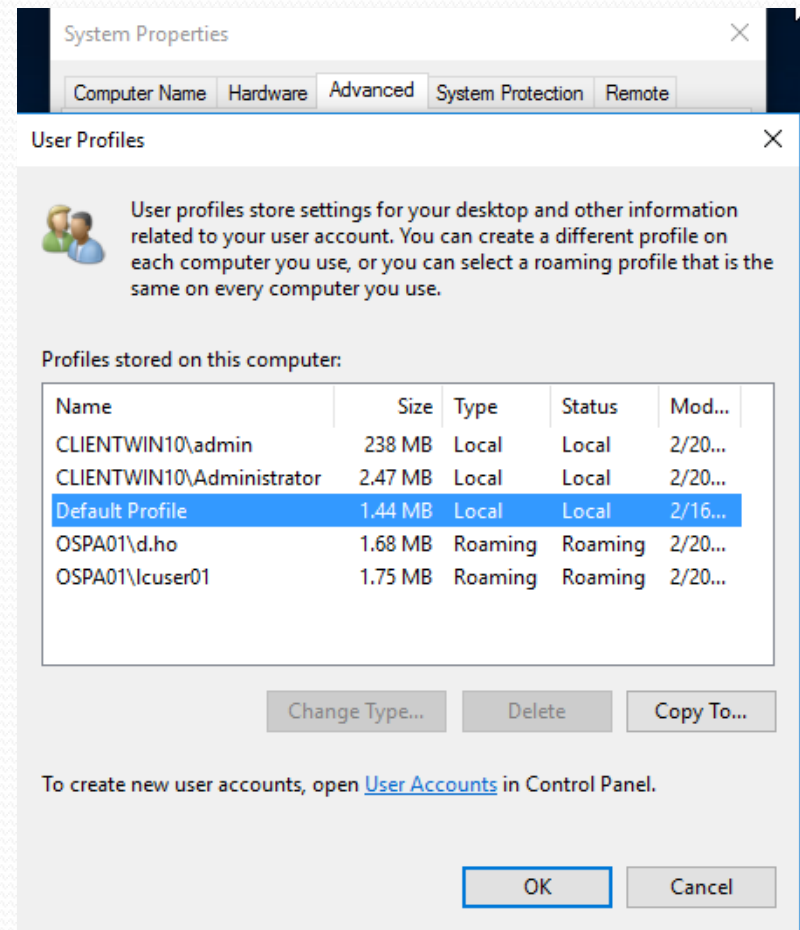
❖ Profiles can be managed in the **User Profiles dialog box**

- Open Control Panel > System
- Click the link “Advanced system settings” on the left
- Click the <Settings...> button under User Profiles section

❖ Three possible actions for **profiles** (*including local and domain users*) **stored locally** (in *C:\Users*)

- **Change Type...** (Roaming or Local)
- **Delete**
- **Copy To...**

❖ **Note:** *Many aspects of user profiles can be managed by using group policies*





# The Cost of Roaming Profiles

- ❖ Windows profiles can become **bloated/bulky/full**
  - Cause **serious problem if they are roaming profiles**
    - If the roaming profile is detected to be newer on the network share than the cached profile on the computer the user is logging in to, the whole profile must be replicated at user logon
    - The reverse is also true if the locally cached profile on the computer should prove to be more up to date at user logoff
    - ➡ **Very long transferring times** in downloading and uploading profiles
- ❖ **Folder redirection** may help in reducing the size of the roaming profiles



# Creating Roaming Profile

1. Create a “Global Security” Group with a name, let’s say *JavaProgrammers*, for those domain users using roaming profiles
2. Create a shared folder for roaming profiles on a server and configure for the following permissions:

Account	Access	Applies to
SYSTEM	Full control	This folder, subfolders and files
Administrators	Full control	This folder only
CREATOR OWNER	Full control	Subfolders and files only
<i>JavaProgrammers</i>	List folder / read data Create folders / append data	This folder only

3. Specify the shared folder in the path information in the Properties dialog box for the user account OR using group policy

# Creating Roaming Profile (cont.)

## 4. Logon a computer using the user account

- A new roaming profile will be created (*if no profile can be found in the share!*)
- The profile is stored inside a folder named using the user's **logon name**
  - **Note:** Each version of Windows comes with a slightly different user profile and they are not always compatible, such folders are therefore added with **different extensions for different Windows versions** in the share!
    - Windows 10 / Server 2016, added with an extension of "V6"
    - Windows 10 (*before ver. 1607*), added with an extension of "V5"
    - Windows 8.1 / Server 2012r2, added with an extension of "V2" or "V4"
    - Windows 8 / Server 2012, added with an extension of "V2" or "V3"
    - Windows 7 / Server 2008r2, added with an extension of "V2"
    - Windows Vista / Server 2008, added with an extension of "V2"
    - Older Windows, like XP, have NO extension

More: <http://larslohmann.blogspot.hk/2015/07/windows-profile-versions.html>

# Creating Roaming Profile (cont.)

- ❖ **Cached roaming profiles and local user profiles** are stored in the logon computer locally in `C:\Users\`
  - If there is no name conflict, the **profile folders** are just using the user's **logon name** (*without any extensions!*)
  - For name conflicts, the profile folder will be created using:
    - user's logon name with an extension of the computer name for local user, e.g. `d.ho.ClientWin10`, `lcuser01.ClientWin81`
    - user's logon name with an extension of the (2nd level) domain name for domain user, e.g. `lcuser01.OSPA01`
  - **Note:** *NO extension .V2, .V5 or etc. will be appeared in the name of local profile folders, they are used in the network profile shares.*

# Creating Roaming Profile (cont.)

❖ To customize a preconfigured **default roaming profile**:

- *Remember: Different Windows systems should have different profiles!*

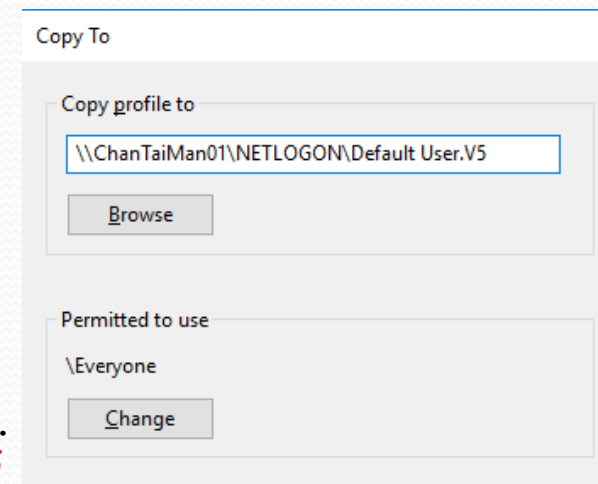
1. Log on to a system as usual using any domain user account
2. Customize the working environment and then log off
3. Log on to the system again with the local Administrator
4. Connect to the domain NETLOGON share
5. Open the User Profiles dialog box

6. Select the profile of the domain user and click <Copy To...>

7. In the Copy To dialog box

- In “Copy profile to”, enter the domain NETLOGON path together with the default user folder name, e.g.  
`\\ChanTaiMan01\NETLOGON\Default User.v5`

- In “Permitted to use”, click <Change>. Enter “**Everyone**” and then click <OK>



More: <https://technet.microsoft.com/en-us/library/cc780839.aspx>

# Creating Mandatory Profile

- ❖ Same as creating roaming profile
  - Because mandatory profile is just a special roaming profile
- ❖ Change ONLY one file extension
  - Rename *NTuser.dat* to *NTuser.man* in the profile directory of the required user in the network profile share
- ❖ Super Mandatory Profile
  - Add one more difference: the profile folder is also required to rename by appending *.man* after the logon name, e.g.  
*d.ho.man.V2*, *lcuser01.man.V5*
  - Then update the profile path of the user account in the DC with “*.man*”, e.g. *\\%LogonServer%\Profile\$\%username%.man*

More: <https://technet.microsoft.com/en-us/library/gg241183.aspx>

# User Groups

---

# Group Accounts



❖ A **group** can be defined as a **collection of accounts** that are grouped together so that administrators can assign permissions and rights to the group as a single entity.

- Simplify the administration of multiple accounts (users, computers, ...)
- Groups in DC
  - TWO types with THREE scopes
- Groups in standalone servers / Windows clients
  - Only ONE kind, stored in the SAM DB

New Object - Group

Create in: ospa01.local/

Group name:  
OSPA\_Users

Group name (pre-Windows 2000):  
OSPA\_Users

Group scope

☐ Domain local  
☒ Global  
☐ Universal

Group type

☒ Security  
☐ Distribution



# Group Accounts (cont.)

## ❖ Security groups

- Created for a collection of accounts who have **the same permissions to resources and the same rights to perform certain system tasks**

## ❖ Distribution groups

- Created to **share information with a group of accounts through e-mails** (*provided AD is integrated with e-mail application, such as Microsoft Exchange*)

## ❖ Group entities can be:

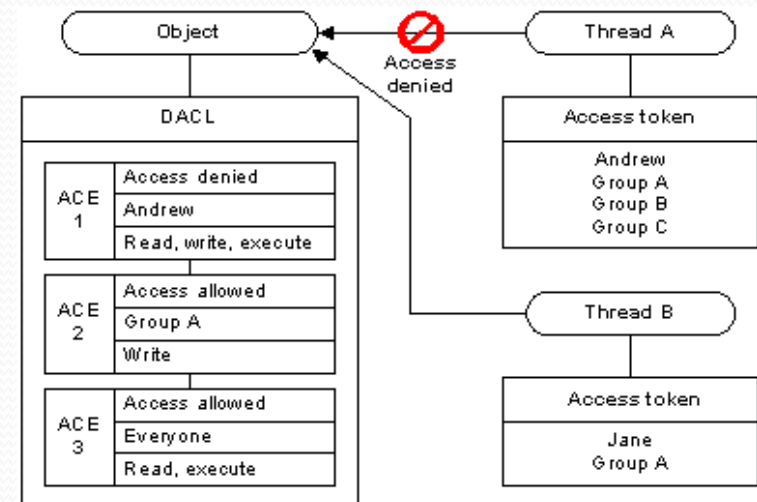
- **User accounts, Computer accounts, Contacts, Other groups**
- **Note:** *If a contact is part of a security group that is assigned permissions to a resource, the contact does not make use of the permissions because a contact is not a **security principal**.*

**Security principals** are any entity that can be authenticated by the OS.



# Converting Group Types

- ❖ Group type can be **changed from Security to Distribution and vice versa**
  - But the conversion is not common
- ❖ Only security groups can be added to a **Discretionary Access Control List (DACL)**
  - If a **security group is converted to a distribution group**, the entry will remain in a DACL. However, it has **NO effect on access to the network resources!**



Ref: <https://msdn.microsoft.com/en-us/library/windows/desktop/aa446597.aspx>

# Group Scopes

- ❖ A group's scope determines where the group can be applied in the forest or the domain, it also determines who can be a member of a group.
- ❖ THREE scopes
  1. Domain Local groups
  2. Global groups
  3. Universal groups

# Group Scopes (cont.)

Group scope	Possible members	Can be a member of	Permissions and rights assignments
Domain local	<div>User accounts, global groups, and universal groups from any domain in the forest</div> <p>Other domain local groups from the same domain</p> <p>User accounts, global groups, and universal groups from trusted domains in another forest</p>	<p>Domain local groups in the same domain</p> <p>Local groups on domain member computers; domain local groups in the Builtin folder can be members only of other domain local groups</p>	Resources on any DC or member computer in <u>the domain</u> ; domain local groups in the Builtin folder can be added to DACLs only on DCs, not on member computers
Global	<div>User accounts and global groups (nested) in the same domain</div>	<p>Global groups in the same domain</p> <p><u>Domain local</u> groups or local groups on member computers in any domain in the forest or trusted domains in another forest</p>	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest
Universal	<p>User accounts, global groups, and universal groups from <u>any domain in the forest</u></p>	<p>Universal groups from any domain in the forest</p> <p>Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest</p>	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest

# 1. Group Scope – Domain Local

- ❖ A Domain Local group is the **main security principal** recommended **for assigning rights and permissions to domain resources**
  - Can have user accounts, computer accounts, Global groups, and Universal groups **from any domain** as group members
  - Can also include other Domain Local groups of the same domain
  - ONLY Domain Local groups can **assign permissions to local resources** OR to **resources that reside in the domain in which the Domain Local group was created**

## 2. Group Scope – Global

- ❖ A main container to group accounts in the domain.
  - Can only have members (*user accounts, computer accounts, and global groups*) **from the domain in which it is created**
  - Usually used to **aggregate users**
  - **Easier to manage** than domain local groups, especially if dealing with an organization that has multiple departments needing access to a single resource
  - Good Practice:
    - Use Global groups to aggregate users and add those groups to Domain Local groups

### 3. Group Scope – Universal

#### ❖ Like Domain Local groups

- Universal groups can have user accounts, computer accounts, Global groups, and other Universal groups **from any domain** in the tree or forest as members
  - Recommended to **add Global groups as members**, NOT individual users

#### ❖ Universal groups' membership information is **stored ONLY on Global Catalog servers**

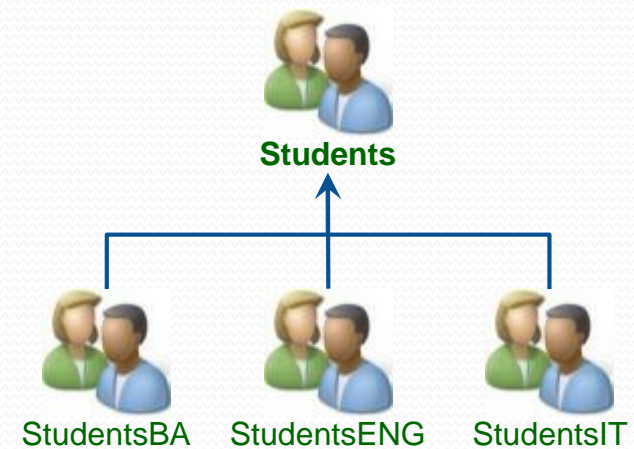
- membership **changes require replication** to all Global Catalog servers

- ***Global Catalog** is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multi-domain forest.*
- ***Global catalog server** is a DC which stores the global catalog which contains universal groups. The membership of other groups can be ascertained at the domain level.*

# Nesting Groups

❖ Group nesting occurs when groups **contain other groups as members.**

- assists in reducing the number of instances that users need to assign permissions and replication traffic
- Group scope's membership rules must be followed
- Usually used to **group users who have similar roles BUT work in different departments**





# Nesting Groups – MS's Best Practice

- ❖ Microsoft's recommendations for implementing role-based access controls in AD
  - In a **single domain** environment, or when users from only one domain are assigned access to a resource, use **AGDLP**
    - user and computer **A**ccounts are members of
    - **G**lobal groups (*sort of account groups*) that represent business roles, which are members of
    - **D**omain **L**ocal groups (*sort of resource groups*) that describe resource **P**ermissions or user rights assignments
  - In **multi-domain** environments where users from different domains are assigned access to a resource, use **AGUDLP**
    - **A**ccounts are made members of
    - **G**lobal groups (*when necessary are nested in other Global groups*) which are made members of
    - **U**niversal groups, which are then made members of
    - **D**omain **L**ocal groups, which are assigned
    - **P**ermissions to resources

More: <http://www.stealthbits.com/company/blog/article/item/163-all-about-agdlp-group-scope-for-active-directory-account-global-domain-local-permissions>



# Converting Group Scopes

- ❖ Group scope can be **converted with some restrictions**
  - **Global cannot contain Universal**
    - Global → Universal
      - provided it is not a member of another global group
    - Universal → Global
      - provided it does not have another universal group as a member
  - **Universal cannot contain Domain Local**
    - Universal → Domain Local
      - provided it is not a member of another universal group
    - Domain Local → Universal
      - provided it does not have another domain local group as a member

# Default Groups in a DC

❖ Container – FIVE Folder Objects created by default:

<b>Builtin</b>	houses <b>default groups</b> and used to <b>assign permissions to users having administrative responsibilities</b> in domain
<b>Computers</b>	default location for computer accounts created when a new <b>computer/server becomes a domain member</b>
<b>ForeignSecurityPrincipals</b>	contains <b>user accounts from other domains added as members</b> of the local domain's groups
<b>Managed Service Accounts</b>	helps to <b>maintain and secure the service accounts</b> used for applications such as <i>SQL Server, Exchange</i>
<b>Users</b>	stores two default <b>users</b> ( <i>Administrator and Guest</i> ) and several default <b>security groups</b>

- CANNOT create new folder objects
- CANNOT apply group policies to folder objects
- Administrative control can be delegated, EXCEPT Builtin folder

# Default Groups in a DC (cont.)

- ❖ Default groups can be found in:
  - Builtin folder
    - Includes are “Security - Domain Local” groups (*most are from the local groups*), for assigning rights and permissions in the local domain
  - Users folder
    - Includes are “Security - Global”, “Security - Universal” and “Security - Domain Local” groups
- ❖ Some other default groups called “Special Identity”
  - Can use to assign rights and permissions
    - These special identity groups do not have specific memberships that can be modified, BUT they can *represent different users at different times, depending on the circumstances*.
    - Although the special identity groups can be assigned rights and permissions to resources, the *memberships CANNOT be modified or viewed*.




















More: <https://technet.microsoft.com/en-us/library/cc756898.aspx>

# Default Groups in Builtin folder

Name	Description
Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Account Operators *	Members can administer domain user and group accounts
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Certificate Service DCOM Access	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of Hyper-V.
IIS_IUSRS	Built-in group used by Internet Information Services.
Incoming Forest Trust Builders *	Members of this group can create incoming, one-way trusts to this forest
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remo...
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Pre-Windows 2000 Compatible Access *	A backward compatibility group which allows read access on all users and groups in the domain
Print Operators	Members can administer printers installed on domain controllers
RDS Endpoint Servers	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group nee...
RDS Management Servers	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated ...
RDS Remote Access Servers	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deploymen...
Remote Desktop Users	Members in this group are granted the right to logon remotely
Remote Management Users	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management...
Replicator	Supports file replication in a domain
Server Operators *	Members can administer domain servers
Terminal Server License Servers *	Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and rep...
Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Windows Authorization Access Group *	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects

\* new groups created after a server is promoted to a DC.

# Default Groups in Users folder

Name	Type	Description
 DnsAdmins	Security Group - Domain Local	DNS Administrators Group
 Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to all read-only domain controllers in the domain
 Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to any read-only domain controllers in the d...
 Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to the directory
 WinRMRemoteWMIUsers__	Security Group - Domain Local	Members of this group can access WMI resources over management protocols (such as WS-Management v...
 RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties of users
 Domain Controllers	Security Group - Global	All domain controllers in the domain
 Domain Guests	Security Group - Global	All domain guests
 Domain Users	Security Group - Global	All domain users
 Domain Computers	Security Group - Global	All workstations and servers joined to the domain
 Domain Admins	Security Group - Global	Designated administrators of the domain
 DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP ...
 Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain
 Protected Users	Security Group - Global	Members of this group are afforded additional protections against authentication security threats. See http...
 Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers in the domain
 Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cloned.
 Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
 Schema Admins	Security Group - Universal	Designated administrators of the schema
 Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the enterprise



# Special Identity Groups

Name
ANONYMOUS LOGON
Authenticated Users
BATCH
CONSOLE LOGON
CREATOR GROUP
CREATOR OWNER
DIALUP
Digest Authentication
ENTERPRISE DOMAIN CONTROLLERS
Everyone
INTERACTIVE
IUSR
LOCAL SERVICE
NETWORK
NETWORK SERVICE
NTLM Authentication
Other Organization
OWNER RIGHTS
PROXY
REMOTE INTERACTIVE LOGON
RESTRICTED
SChannel Authentication
SELF
SERVICE
SYSTEM
TERMINAL SERVER USER
This Organization

- ← Any user who accesses the system through a sign-in process has the Authenticated Users identity. This identity allows access to shared resources within the domain, such as files in a shared folder that should be accessible to all the workers in the organization.
- ← The person who created the file or the directory is a member of this special identity group. Windows OS uses this identity to automatically grant access permissions to the creator of a file or directory.
- ← All interactive, network, dial-up, and authenticated users are members of the Everyone group. This special identity group gives wide access to system resources. Whenever a user logs on to the network, the user is automatically added to the Everyone group.
- ← The Windows OS itself.

More: <https://technet.microsoft.com/en-us/library/dn617202.aspx>

# Local Groups in Standalone Windows

- ❖ In Windows clients and standalone servers (*before promoting to a DC*), user accounts and groups are considered as “local”
  - only have access to resources on the local computer and nothing else

Account	In Windows clients & standalone servers, it is...	After promoting to a DC, it is...
<b>Administrator</b>	<ul style="list-style-type: none"> <li>• a member of the (<i>local</i>) <b>Administrators</b> group by default</li> </ul>	<ul style="list-style-type: none"> <li>• added to <b>Domain Admins</b> global security group</li> </ul>
<b>Guest</b>	<ul style="list-style-type: none"> <li>• a member of the (<i>local</i>) <b>Guests</b> group by default</li> <li>• disabled by default</li> </ul>	<ul style="list-style-type: none"> <li>• added to <b>Domain Guests</b> global security group</li> <li>• <i>unable to logon to the DC directly</i></li> </ul>
<i>Other user created locally</i>	<ul style="list-style-type: none"> <li>• a member of the (<i>local</i>) <b>Users</b> group by default</li> </ul>	<ul style="list-style-type: none"> <li>• added to <b>Domain Users</b> global security group</li> <li>• <i>unable to logon to the DC directly</i></li> </ul>
Group	In Windows clients & standalone servers, ...	After promoting to a DC, ...
<i>local builtin groups</i>	<ul style="list-style-type: none"> <li>• 22 local groups</li> <li>• including “<b>Power Users</b>” for backwards compatibility (<i>have limited administrative powers</i>)</li> </ul>	<ul style="list-style-type: none"> <li>• all moved under the <b>builtin</b> folder</li> <li>• “<b>Power Users</b>” are removed</li> <li>• 6 more new groups are added</li> </ul>

reside in SAM DB

reside in AD DB



# Computer Accounts

---

# Computer Accounts

- ❖ **Computer accounts** are created in AD when a computer joins as a domain member
  - Like a user account, a computer account is also a security principal and has an associated password to logon to the DC
  - **Administrators cannot manage such password**, instead, the password will **change automatically in every 30 days**  
⇒ may cause synchronization issues if a computer is left off for too long

# Computer Accounts (cont.)

## ❖ Advantages in having member computers

- Single Sign-on (SSO)
  - users can access to any permitted resources throughout the forest using only one set of credentials without needing to authenticate again
- AD Search
  - logon users can search AD for objects and resources throughout the forest
- Group Policies
  - administrators can manage member computers by using group policies
- Remote Management
  - administrators can manage member computers remotely through different MMC snap-ins



# Account Management

---

# Managing AD Objects

## ❖ Windows **net** commands

### • **net group** /?

- NET GROUP *JavaProgrammers* /ADD /COMMENT:"*Java Programmers (Global Security)*"
- NET GROUP *JavaProgrammers* /DELETE

### • **net localgroup** /?

- NET LOCALGROUP *IT* /ADD /COMMENT:"*IT Division (Domain Local Security)*"
- NET LOCALGROUP *IT Programmers* /ADD
- NET LOCALGROUP *IT* /DELETE

### • **net user** /?

- NET USER *d.ho Pa\$\$w0rd* /ADD /FULLNAME:"*Don E. Ho*"
- WMIC USERACCOUNT WHERE "Name='*d.ho*'" SET PasswordExpires=FALSE
- NET GROUP *Programmers d.ho* /ADD
- NET USER *d.ho* /DELETE

### • **net computer** /?

- NET COMPUTER *\\ClientWin10* /ADD
- NET COMPUTER *\\ClientWin10* /DEL

### • **net view** /?

- NET VIEW *\\ChanTaiMan01*

### • **net use** /?

- NET USE *Z: \\ChanTaiMan01\NETLOGON* /USER:*mary Pa\$\$w0rd*
- NET USE *Z:* /DELETE

More: <https://technet.microsoft.com/en-us/library/cc754340.aspx>

# Managing AD Objects (cont.)

## ❖ Directory service commands

### • dsadd /?

- DSADD **USER** CN=aduser01,CN=Users,DC=ospa,DC=local -UPN aduser01@ospa.local -DISPLAY "AD User 01" -PWD Pa\$\$w0rd -PWDNEVEREXPIRES YES -DISABLED NO
- DSADD **OU** OU=OSPA\_Users,DC=ospa,DC=local -DESC "OSPA Users"
- DSADD **GROUP** CN=JavaProgrammers,OU=OSPA\_Users,DC=ospa,DC=local -SECGRP YES -SCOPE G -DESC "Java Programmers (Global Security)"
- DSADD **GROUP** CN=CodingTeam,OU=OSPA\_Users,DC=ospa,DC=local -SECGRP YES -SCOPE U -DESC "Coding Team (Universal Security)" -MEMBERS JavaProgrammers
- DSADD **GROUP** CN=IT,OU=OSPA\_Users,DC=ospa,DC=local -SECGRP YES -SCOPE L -DESC "IT Division (Domain Local Security)" -MEMBERS CodingTeam
- DSADD **USER** CN=d.ho,OU=OSPA\_Users,DC=ospa,DC=local -UPN d.ho@ospa.local -FN Don -MI E -LN Ho -DISPLAY "Don E. Ho" -PWD Pa\$\$w0rd -PWDNEVEREXPIRES YES -DISABLED NO -PROFILE %LogonServer%\Profile\$\%username% -LOSCR %LogonServer%\NetLOGON\login.vbs -HMDRV Z: -HMDIR \\ChanTaiMan01\Home\$\d.ho
- DSADD **COMPUTER** CN=ClientWin10,CN=Computers,DC=ospa,DC=local

### • dsrm /?

- DSRM CN=ClientWin10,CN=Computers,DC=ospa,DC=local -NOPROMPT
- DSRM CN=aduser01,CN=Users,DC=ospa,DC=local -NOPROMPT
- DSRM OU=OSPA\_Users,DC=ospa,DC=local -SUBTREE -NOPROMPT

### • dsmod /?

- DSMOD **USER** CN=aduser01,CN=Users,DC=ospa,DC=local -PWD A1b2C3d4 -MUSTCHPWD YES

### • dsmove /?, dsquery /?, dsget /?

More: <https://technet.microsoft.com/en-us/library/cc754340.aspx>

# Managing AD Objects (cont.)

- ❖ Two more important directory service commands
  - `csvde /?` and `ldifde /?`
    - Two tools to create snapshots of the Active Directory DB
    - Bulk import and export information using Plain Text files (`.csv` or `.ldf`)
    - Limitation: NOT work with passwords in both import/export
  - Comma Separated Value Directory Exchange (CSVDE)
    - CSV files are easy to read and use
    - Can only be used to create new objects
  - LDAP Data Interchange Format Directory Exchange (LDIFDE)
    - LDIF files are in a cross-platform standard
    - Allow for creation, modification and deletion of objects
    - Not support changing group membership



# Using CSVDE

❖ CSV files have a **header row listing attributes** of the AD object

- All data are separated by a comma (,)

➤ CSVDE -F *OutFile1.csv*

➤ CSVDE -D OU=*OSPA\_Users*,DC=*ospa*,DC=*local* -F *OutFile2.csv*

```
DN,objectClass,distinguishedName,instanceType,whenCreated,whenChanged,subRefs,uSNCreated,.....
"DC=ospa,DC=local",domainDNS,"DC=ospa,DC=local",5,20160215184412.0Z,20160226204817.0Z,....
"CN=Users,DC=ospa,DC=local",container,"CN=Users,DC=ospa,DC=local",4,20160215184436.0Z,....
"CN=Administrator,CN=Users,DC=ospa,DC=local",user,"CN=Administrator,CN=Users,DC=ospa,DC=.....
"CN=Guest,CN=Users,DC=ospa,DC=local",user,"CN=Guest,CN=Users,DC=ospa,DC=local",4,.....
.....
```

➤ CSVDE -I -K -F *InFile.csv*

- As no password can be set, all user accounts created are **disabled** and **user must change password at next login**

```
DN,objectClass,sAMAccountName,userPrincipalName
"CN=aduser01,CN=Users,DC=ospa,DC=local",user,aduser01,aduser01@ospa.local
```

```
DN,objectClass,sAMAccountName,userPrincipalName,givenName,initials,sn,displayName,profilePath,scriptPath,homeDrive,homeDirectory
"CN=d.ho,OU=OSPA_Users,DC=ospa,DC=local",user,d.ho,d.ho@ospa.local,Don,E,Ho,Don E. Ho,
\\%LogonServer%\Profile$\%username%,\\%LogonServer%\NetLOGON\login.vbs,Z:,%LogonServer%\Home$\%username%
```

# Using LDIFDE

❖ Usages are the same as CSVDE, only the file format (LDIF) is different

- Has line-separated values for a record
- Has a blank line between each record

➤ LDIFDE -F *OutFile1.ldf*

➤ LDIFDE -D OU=*OSPA\_Users*,DC=*ospa*,DC=*local* -F *OutFile2.ldf*

➤ LDIFDE -I -K -F *InFile.ldf*

- Existing AD objects can be modified (*changetype: modify*) or deleted (*changetype: delete*)
- ONLY one attribute value can be modified in a record of instructions
- A hyphen (-) must be appended for the modification action of the record of instructions

```
dn: OU=OSPA_Users,DC=ospa,DC=local
changetype: add
objectClass: top
objectClass: organizationalUnit
ou: OSPA_Users
description: OSPA Users
instanceType: 4
whenCreated: 20160227020458.0Z
whenChanged: 20160227020458.0Z
uSNCreated: 49206
.....
```

```
dn: CN=aduser01,CN=Users,DC=ospa,DC=local
changetype: modify
replace: homeDrive
homeDrive: Z:
-

dn: CN=aduser01,CN=Users,DC=ospa,DC=local
changetype: modify
replace: homeDirectory
homeDirectory: \\ChanTaiMan01\Home$\aduser01
-

dn: CN=aduser02,CN=Users,DC=ospa,DC=local
changetype: delete

dn: CN=d.ho,OU=OSPA_Users,DC=ospa,DC=local
changetype: delete
```

# Using LDIFDE (cont.)

- Changing password is feasible but not trivial

➤ LDIFDE -I -K -F *InFile.ldf* -H

➔ Password changing requires execution through SASL (Simple Authentication and Security Layer)

```
dn: CN=d.ho,OU=OSPA_Users,DC=ospa,DC=local
changetype: modify
replace: unicodePwd
unicodePwd::IgBQAGEAJAAkAHcAMABYAGQAIgA=
-
```

➔ "Pa\$\$w0rd" is encoded using Base64 (UTF-16)

```
dn: CN=d.ho,OU=OSPA_Users,DC=ospa,DC=local
changetype: modify
replace: userAccountControl
userAccountControl: 66080
-
```

➔ Password never expires & Account is enabled

More: <https://support.microsoft.com/en-us/kb/263991>  
<http://www5.rptea.com/base64>

# Managing AD Objects (cont.)

## ❖ Legacy scripting language – **VBScript**

- Can manage computers that cannot run PowerShell
- VBScript is “lighter” than PowerShell, utilizes less memory

```
Option Explicit
Dim strUser, objRoot, objContainer, objUser
Const ADS_UF_DONT_EXPIRE_PASSWD = &H10000
strUser = "d.ho"
Set objRoot = GetObject("LDAP://rootDSE")
Set objContainer = GetObject("LDAP://ou=OSPA_Users," & objRoot.Get("defaultNamingContext"))

Set objNewUser = objContainer.Create("User", "cn=" & strUser)
objUser.Put "sAMAccountName", strUser
objUser.Put "givenName", "Don"
objUser.Put "initials", "E"
objUser.Put "sn", "Ho"
objUser.Put "displayName", "Don E. Ho"
objUser.SetInfo

objUser.SetPassword "Pa$$w0rd"
objUser.Put "userAccountControl", ADS_UF_DONT_EXPIRE_PASSWD
objUser.AccountDisabled = False
objUser.SetInfo
WScript.Quit
```

# Summary

- ❖ Three categories of users in Windows
  - local, domain, builtin
- ❖ User account names
  - unique in a domain
  - case insensitive
  - Better to use 20 or fewer characters (*limitation for old clients*)
  - Should have a consistent and standard of naming
- ❖ User account passwords are required “complex” by default
  - configure in **Local Security Policy, Default Domain Policy**
- ❖ **User templates**, *are just disabled user accounts*, facilitate creating users who have some attributes in common, such as *group memberships*

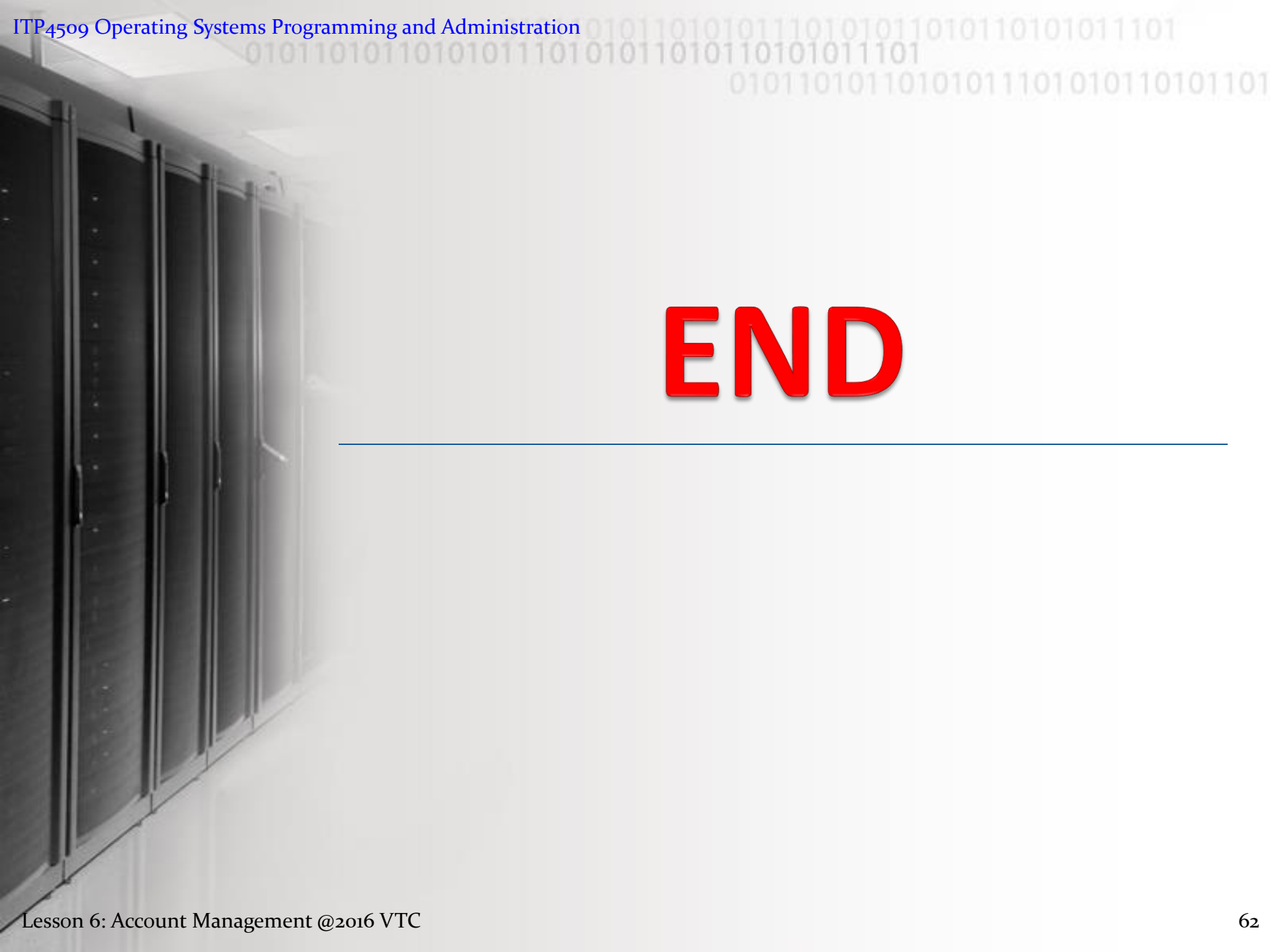
# Summary (cont.)

- ❖ Each Windows user must have a **user profile** in using a Windows OS
  - A user profile contains
    - personal files and
    - computer settings that define the user's environment
  - A user profile stored on a network share is called a **roaming profile**
    - can be made **mandatory** OR **super-mandatory**
- ❖ User **groups** are the primary security principal used to grant rights and permissions

# Summary (cont.)

- ❖ In AD, DCs manage all AD objects
  - Computer accounts
    - will be created automatically when a computer joins a domain as domain members OR
    - can be created manually by an administrator
  - Two group types: Security, Distribution
  - Three group scopes: **G**lobal, **U**niversal, **D**omain **L**ocal
    - Recommended use of groups: **AGDLP**, **AGUDLP**
  - **O**rganizational **U**nits, are very similar to groups BUT they are mainly used for applying group policies
- ❖ Account management can be automated by Batch Commands, VBScripts or **PowerShell Scripts**





# END

---