

Introducing Active Directory

Lesson 5

Agenda

- ❖ Describe the **role** of a directory service and the physical and logical **Active Directory (AD)** structure
- ❖ Install AD
- ❖ Describe the main **AD objects**
- ❖ Configure and apply **group policies**

What is a Directory?

- ❖ Originally, it is a book listing individuals or organizations globally in details such as *names, addresses and telephone numbers in alphabetical order*. (*Yellow Pages*)
- ❖ A **specialized database** designed for storage, retrieving and viewing data such as *text, images, URLs, user accounts, etc.*
- ❖ Also called “**folder**” by MS, works like a filing cabinet of a data-storage device (*disk, CD, DVD*) in which data (*as files*) is grouped and listed in a hierarchical structure.
 - The top most directory is called the “**root directory**” which can, and often has lower level directories called **sub-directories** which too can have their own sub-directories, and so on.

Directory Service

- ❖ A network OS service, a software system, a central information repository, a centralized management tool
 - **stores and organizes network resources** such as *user accounts, email addresses, peripheral devices and computers*, and makes these resources **accessible to users and applications**
 - functions as a **single point** which users can **locate resources distributed** throughout the network
 - also gives administrators a **single point for managing** its objects
- ❖ Virtually all directory services are based on the X.500 ITU standard, e.g. *LDAP, NDS (Netware Directory Service)*

Microsoft Active Directory

- ❖ Active Directory (AD) is a directory service from Microsoft
 - was initially released with Windows Server 2000
 - stores information in hierarchical tree like structure
 - depends on using Domain Naming System (DNS) and Lightweight Directory Access Protocol (LDAP) for information queries and Kerberos V5 for authentication
 - provides a common interface for organizing and maintaining network resources
 - serves as a single data store for quick data access to all users and controls access to users based on the security policy set by the administrator

DNS and LDAP

❖ Domain Naming System (DNS)

- A hierarchical naming and domain name resolution system used on Internet and Windows network for naming resolution.
 - converts the domain name into its related IP address

❖ Lightweight Directory Access Protocol (LDAP)

- A directory access protocol which is used to exchange directory information from server to clients or from server to server.
 - default port number is 389

Microsoft Active Directory (cont.)

- ❖ AD allows Windows clients connected and referenced to a common database that stored on a server for usernames and passwords
- ❖ Then corresponding settings will be applied to the connected clients based on information programmed by the administrator
- ❖ Users only use one set of credentials for all network resources
- ❖ Administrators can control every aspect of connected clients and users

Microsoft Active Directory (cont.)

❖ Adv.

- One set of permissions for the whole organization
- Single sign on
- Task automation
- Better security

❖ Disadv.

- Connected computers become part of a greater whole domain
- Permissions and settings are inherited from the domain server
- Computer will behave differently if disconnected from the domain

Five Roles of AD Services

❖ AD Domain Services (DS)

- An X.500-based directory service that provides integrated authentication and authorization services for a Windows computing environment.

❖ AD Lightweight Directory Services (LDS)

- A stripped down version of AD DS that focuses on providing just the directory services functionality.

❖ AD Federation Services (FS)

- A web services-based technology for providing web single sign-on authentication services between different organizations.

❖ AD Certificate Services (CS)

- Provides digital certification enrollment and revocation services in the support of a Public Key Infrastructure (PKI).

❖ AD Rights Management Services (RMS)

- Provides a solution for managing how users can use documents that they're authorized to access.

Overview of the Structure of AD

❖ Physical structure

- consists of **Sites** and servers configured as **Domain Controllers (DC)**

❖ Logical structure

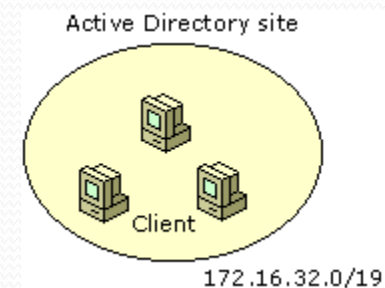
- depicts the directory service's look and feel by
 - **Organizational Unit (OU)**
 - **Domain**
 - **Tree**
 - **Forest**

More: <https://technet.microsoft.com/en-us/library/cc782048.aspx>

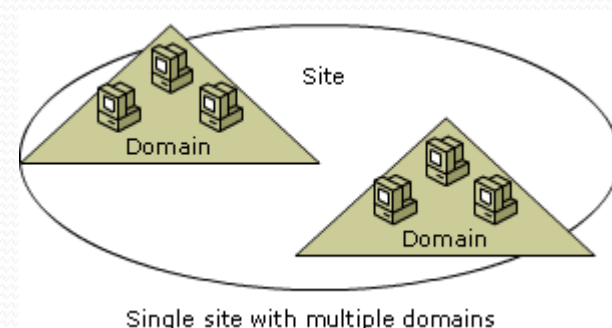
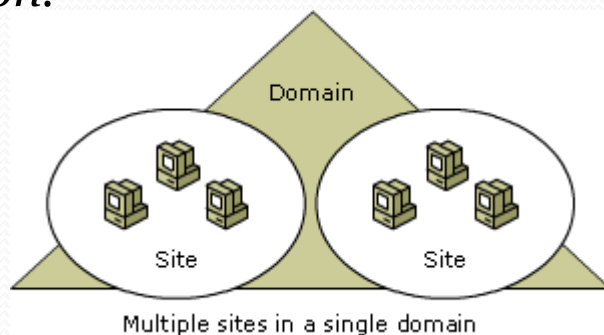
AD's Physical Structure – Site

❖ **Site** is a physical location, simply a collection of **well-connected computers** by a high-speed network, e.g. *LAN*.

- physical (rather than logical) grouping of one or more IP **subnets** who share the common LAN connectivity without knowing the actual physical location of computers is called site.



- Sites differ from domains: *Sites represent the physical structure of your network, while domains represent the logical structure of your organization.*



AD's Physical Structure – DC

- ❖ Domain Controller (DC) is a computer running Windows Server with AD service.
 - Each DC can support maximum one domain.
 - It is always advised to have more than one DC in a domain.
 - DCs communicate and replicate information regularly
 - Each DC is responsible for the following functions:
 - Storing a copy of the domain data and replicating changes to that data to all other DCs throughout the domain
 - Providing data search and retrieval functions for users attempting to locate objects in the directory
 - Providing authentication and authorization services for users who logon to the domain and attempt to access network resources

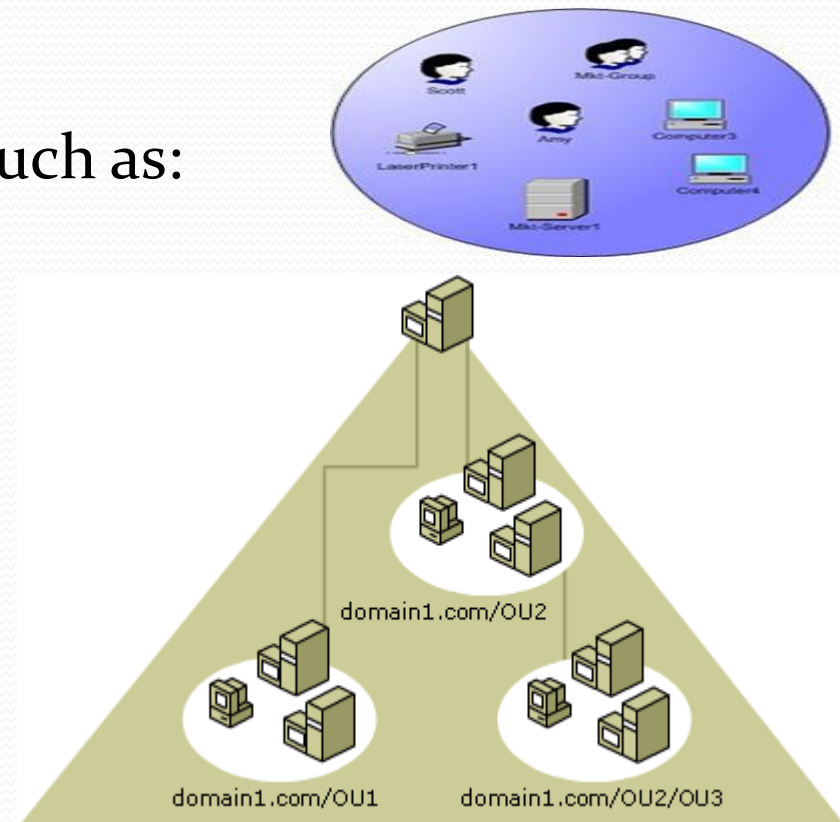
AD's Logical Structure – OU

❖ **Organizational Unit (OU)** is an AD **logical container** used to **organize network resources in a domain** for administrative purposes

- An OU contains AD objects, such as:

- *User accounts, Groups*
- *Computer accounts, Servers, DCs*
- *Applications, Shared folders*
- *Printers*

- Cannot contain objects from other domains
- Can contain other OUs



More: <https://technet.microsoft.com/en-us/library/cc758565.aspx>

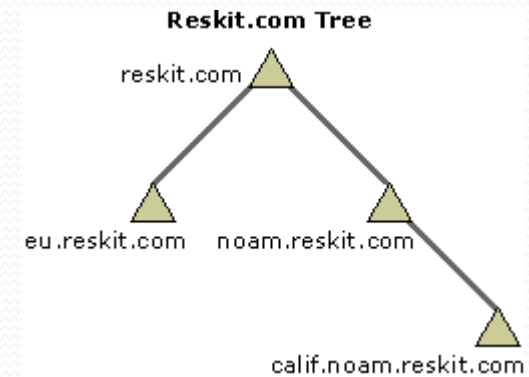
AD's Logical Structure – Domain

- ❖ **Domain** is the core unit of logical structure in AD
 - stores information about all network objects that belong to the same domain in a single DB (*which can be replicated*)
 - contains **OUs** and represents administrative, security, and policy boundaries
 - All security policies and settings, such as *administrative rights, security policies, and Access Control Lists*, do not cross from one domain to another.
- ❖ **Domain Administrator** has full rights to set policies *only within domain they belong to*.
- ❖ Small to medium companies usually have one domain
- ❖ Large companies may have several domains to *separate geographical regions or administrative responsibilities*

More: <https://technet.microsoft.com/en-us/library/cc780856.aspx>

AD's Logical Structure – Tree

- ❖ **Tree** is a collection of **one or more AD domains** that share a **common DNS namespace** and domains are linked in a **2-way transitive trust hierarchy**.
 - has a single root domain
 - each domain below the **root domain** has exactly one superior or **parent domain**
 - a (parent) domain can consists of one or more **child domains**
- ❖ *Domains are created below the root domain to **minimize AD replication** and to provide a means for creating domain names that do not change.*
- ❖ *Administrative **privileges do not extend** from parent domains to child domains.*



AD's Logical Structure – Forest

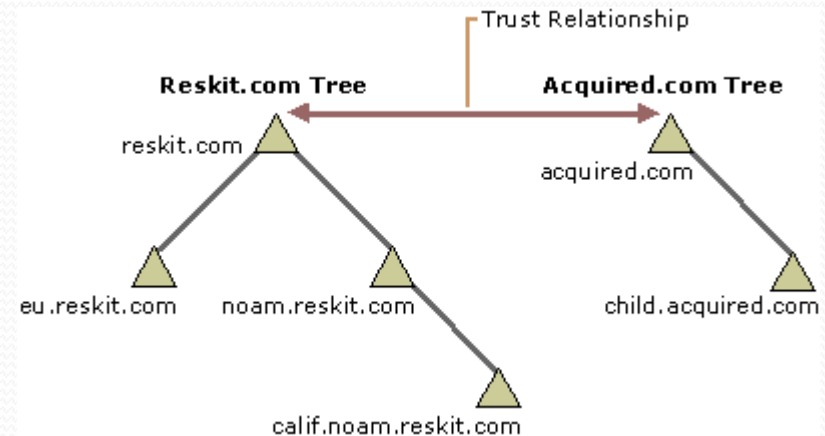
❖ **Forest** is a collection of **one or more AD trees**, organized as peers and connected by usually 2-way transitive trust relationships

- can consist of just one single tree with a single domain

- trees in the same forest do not form a contiguous namespace

- **all domains in all trees can communicate and share information**, while simultaneously **allowing independent operation and administration**


- The first domain created in a forest is called the **forest root domain**





Install Active Directory

Installing Active Directory

- ❖ Use **Server Manager** to install AD on a Windows Server
 - If DNS is not already present on the network, we must install the **DNS Server** role first
 - Then we add the **Active Directory Domain Services** role
 - Finally start the **Domain Controller (DC)** setup
 - Open Server Manager. In the top right menu, click the **Task flag**  and then the link “**Promote this server to a domain controller**” to start the AD DS Configuration Wizard
 - *In the old server versions, we can simply execute **dcpromo.exe***

More: <http://www.rebeladmin.com/2014/07/step-by-step-guide-to-setup-active-directory-on-windows-server-2012>
https://technet.microsoft.com/en-us/library/hh472162.aspx#BKMK_GUI

Installing Active Directory (cont.)

❖ AD DS Configuration Wizard steps:

1. Existing domain or new domain
2. Fully Qualified Domain Name (FQDN) for new forest's root domain name, e.g. *microsoft.com*, *vtc.edu.hk*, *ospa.local*
3. Choose functional level of the new forest and root domain
 - The functional level is critical to the feature set available to administrators after install, as well as the software requirements for any other DCs, default is **Windows Server 2012r2**
 - For backwards compatibility with older DCs on the network, choose Windows Server 2008, 2008r2 or 2012 for forest functional level
 - **Note:** *choosing Windows Server 2012r2 functional level, you can't run DC other than Windows Server 2012r2, but servers with older versions can be run as member servers*

More: <http://go.microsoft.com/fwlink/?LinkId=219492>

Installing Active Directory (cont.)

4. Specify DC capabilities (THREE functions):

- Domain Naming System (DNS) server
 - globally distributed DB that resolves domain names and IP addresses
 - default for the 1st DC with DNS in a new domain
- Global Catalog (GC) *More: <https://technet.microsoft.com/en-us/library/cc728188.aspx>*
 - contains full information of all network objects in its own domain and partial information of objects in other domains
 - default for the 1st DC in a forest
- Read Only Domain Controller (RODC)
 - RODCs are additional DCs for a domain that host complete, read-only copies of the partitions of the AD database and a read-only copy of the SYSVOL folder contents.
 - not available for the 1st DC in a new domain

5. Set the Directory Services Restore Mode (DSRM) password

More: <http://www.top-password.com/knowledge/reset-directory-services-restore-mode-password.html>

Installing Active Directory (cont.)

6. Additional DNS or RODC options

- not available for the 1st DC in a new domain

7. Verify the NetBIOS domain name

8. Specify the location of the AD DS database

(*%SystemRoot%\NTDS*), log files (*%SystemRoot%\NTDS*) and SYSVOL (*%SystemRoot%\SYSVOL*)

- Database name is **NTDS.DIT**, contains the schema, global catalog and objects stored in a DC
- **SYSVOL**, the **system volume** shared directory on the DC, **stores the information from AD that must be shared for common access and replication to other DCs throughout a domain**

```
Import-Module ADDSDeployment

Install-ADDSForest -CreateDnsDelegation:$false `
  -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" `
  -DomainName "ospa.local" -DomainNetbiosName "OSPA" `
  -ForestMode "Win2012R2" -InstallDns:$true -LogPath "C:\Windows\NTDS" `
  -NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -Force:$true
```

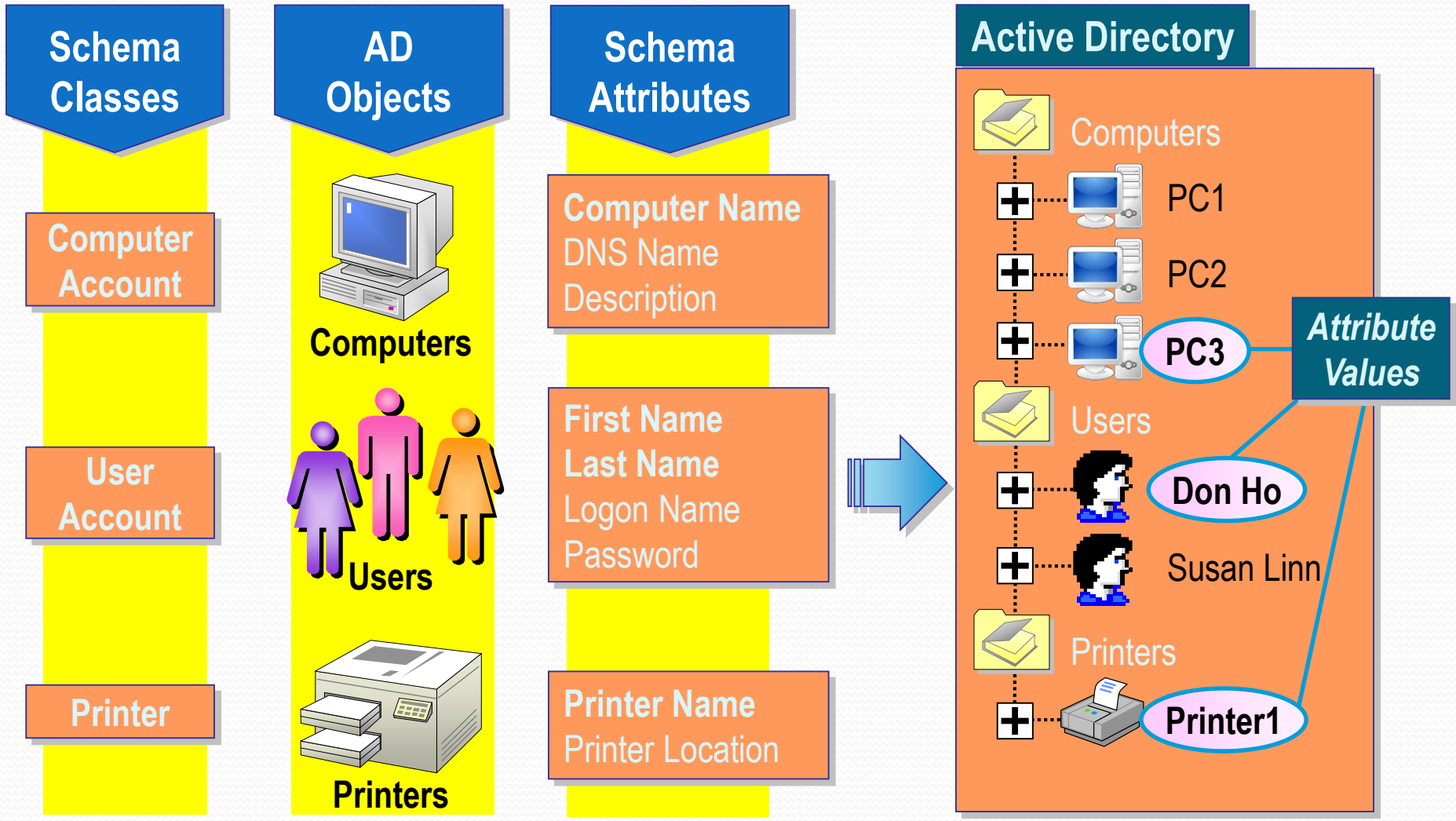


Active Directory Objects

AD Objects

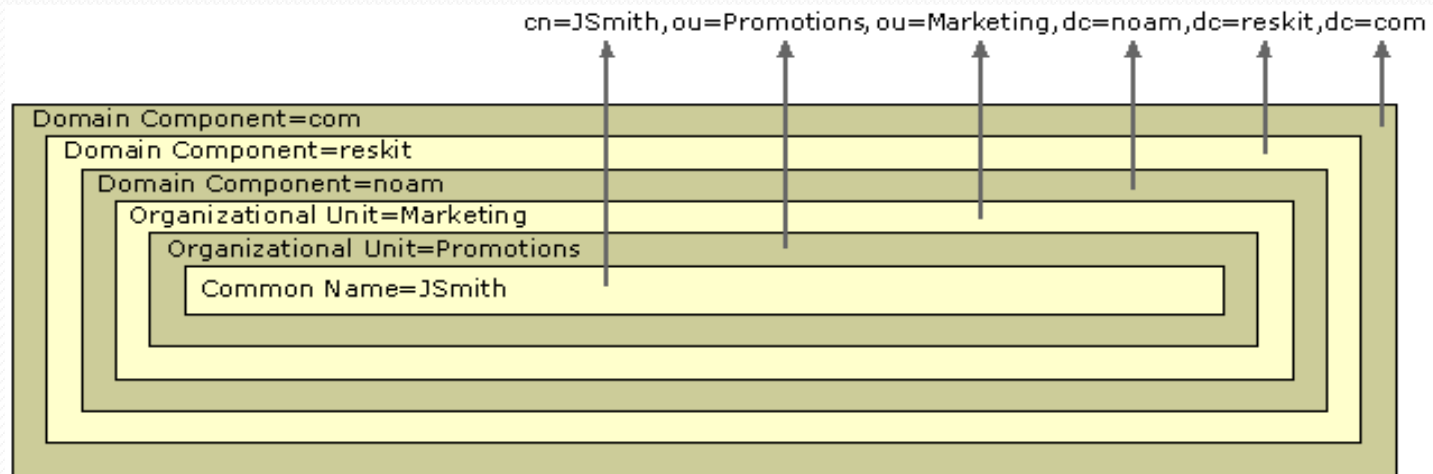
- ❖ Data stored in AD is organized into **objects**
 - An object is a **network resource**
 - An object is an **instance of storage of a class**
 - A class is **defined in the AD schema**
- ❖ **Schema** defines the type, organization, and structure of data stored in the AD database
 - **Only one** consistent Schema for the entire Forest
 - **Schema classes** define the types of objects to be stored in AD
 - Classes are inherited
 - **Schema attributes** are specified in classes (**optional or mandatory**), define what type of information is stored in each object
 - The information stored in each attribute is called the **attribute value**

AD Schema



AD Object Naming

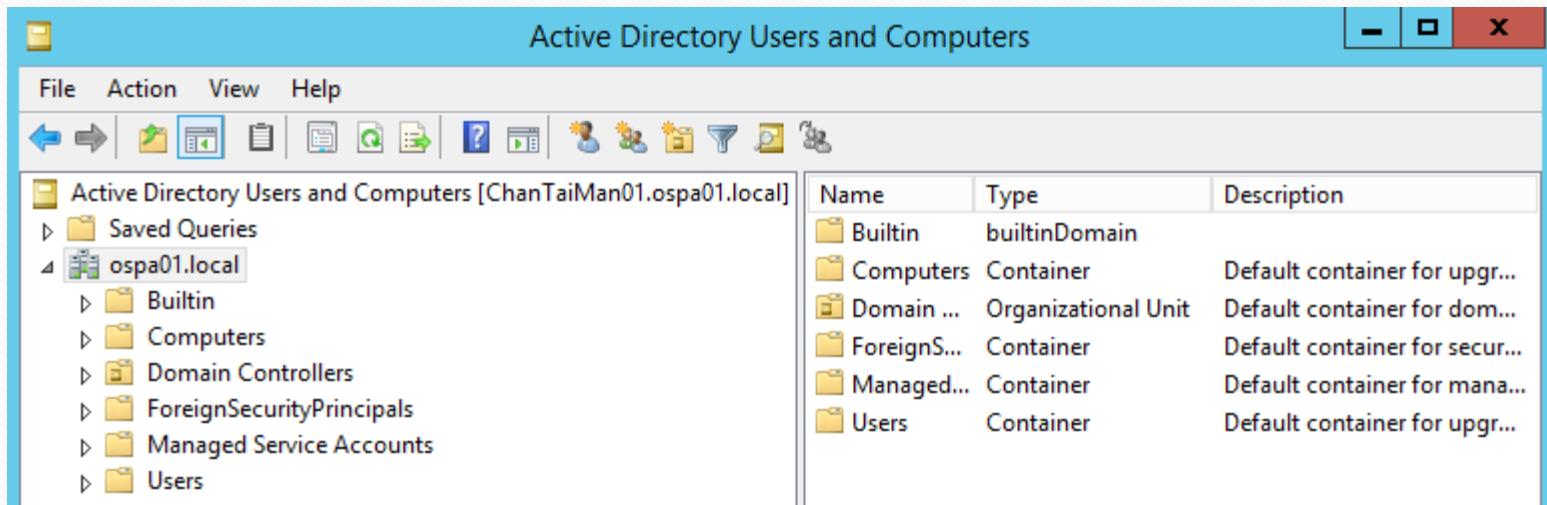
- ❖ AD is an LDAP-compliant directory service
 - LDAP requires that names of directory objects be standardized formed
 - AD objects are located within domains according to a hierarchical path
 - The full path to an object is defined by **D**istinguished **N**ame (**DN**)
 - For example: *User “Jsmith” works in the North American branch of the company. The root domain of the company is reskit.com, and the local domain is noam.reskit.com*




More: <https://technet.microsoft.com/en-us/library/cc977992.aspx>

AD Container Objects

- ❖ “Container” refers to one of two things:
 - An object of the *container structural class*
 - An object that **has child objects**
 - *Organizational Units, Folder Objects, Domain Objects*
- ❖ Explore using Active Directory Users and Computers MMC



Container – Organizational Units

- ❖ Primary container object 
 - “Domain Controller” is the default OU created
 - for **organizing and managing resources** in a domain
 - can organize multiple objects into ONE **administrative group** that can be **configured with specific group policies**
 - Administrative control can be **delegated** to a user
- ❖ Typical object types in an OU include *user accounts, group accounts, computer accounts, shared folders, shared printers, published applications, and other OUs*
- ❖ **Nesting OUs** can build a hierarchical AD structure that **mimics the corporate structure for easier object management**


Container – Folder Objects

❖ Only FIVE, created by default: 

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

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

Container – Domain Objects

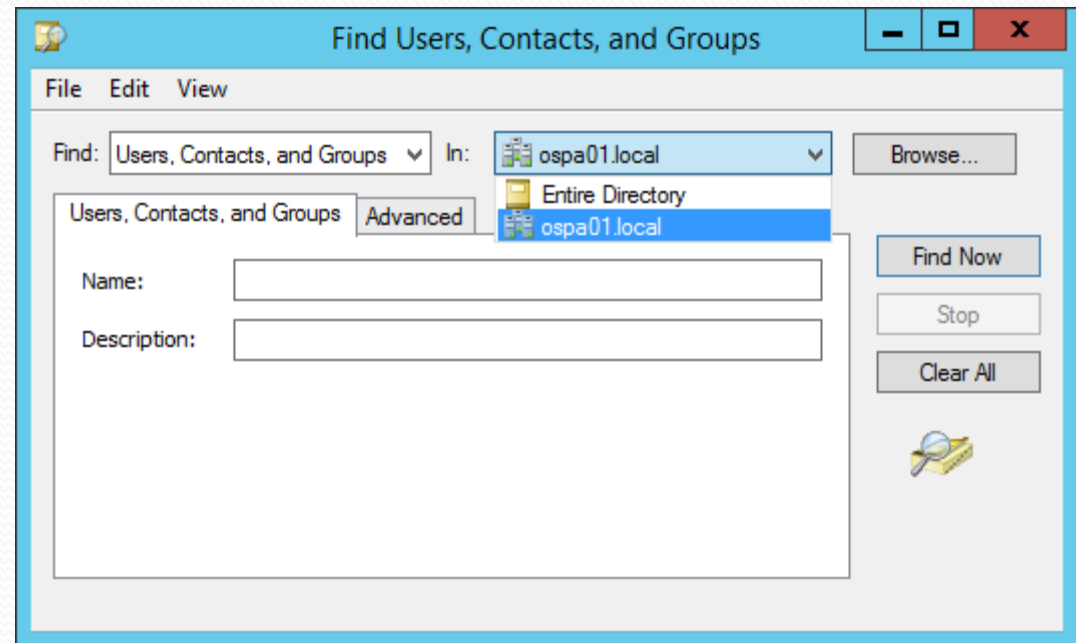
- ❖ Core logical structure in AD 
 - contains **OU** and **Folder** container objects, as well as **leaf objects** (*those have NO child object, such as users, groups*)
- ❖ Larger companies may use multiple domains to **separate administration, define security boundaries, and define policy boundaries**
- ❖ Each **domain** object has a default **Group Policy Object** (**GPO**) linked to it that can **affect all objects in that domain**

AD Leaf Objects

- ❖ A leaf object does not contain other objects
 - **User Accounts**
 - 3 types: **local users**, **domain users**, built-in users
 - **Groups**
 - consist of users with common permissions
 - **Computer Accounts**
 - represent computers that are **DCs** or **domain members**
 - **Others**
 - Printer, Shared Folder, GPO,

Locating AD Objects

- ❖ AD objects can be searched for using the “Find Users, Contacts, and Groups” dialog box
 - Right click a domain and select “Find...” in Active Directory Users and Computers MMC
 - Can search a single domain or an entire directory (all domains)
 - Not all objects are available to all users



Group Policies

Introducing Group Policies

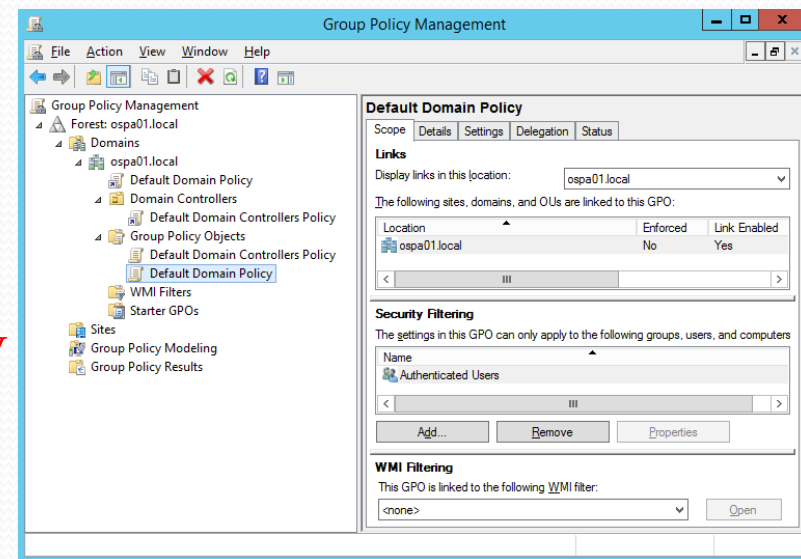
❖ A **Group Policy Object (GPO)** is a list of **settings that administrators use to configure user and computer operating environments** remotely

❖ TWO default GPOs created in installing AD:

1. Default Domain Policy
2. Default Domain Controllers Policy

❖ Managing GPO

- Using **Group Policy Management Console (GPMC)**, a MMC snap-in, `gpmc.msc`
 - Server Manager > Tools > Group Policy Management
- Setting local computer policy, `gpedit.msc`



More: <https://mizitechinfo.wordpress.com/2013/08/06/simple-guide-implementing-group-policy-in-windows-server-2012-r2>

Introducing Group Policies (cont.)

❖ TWO divisions/nodes for every GPO

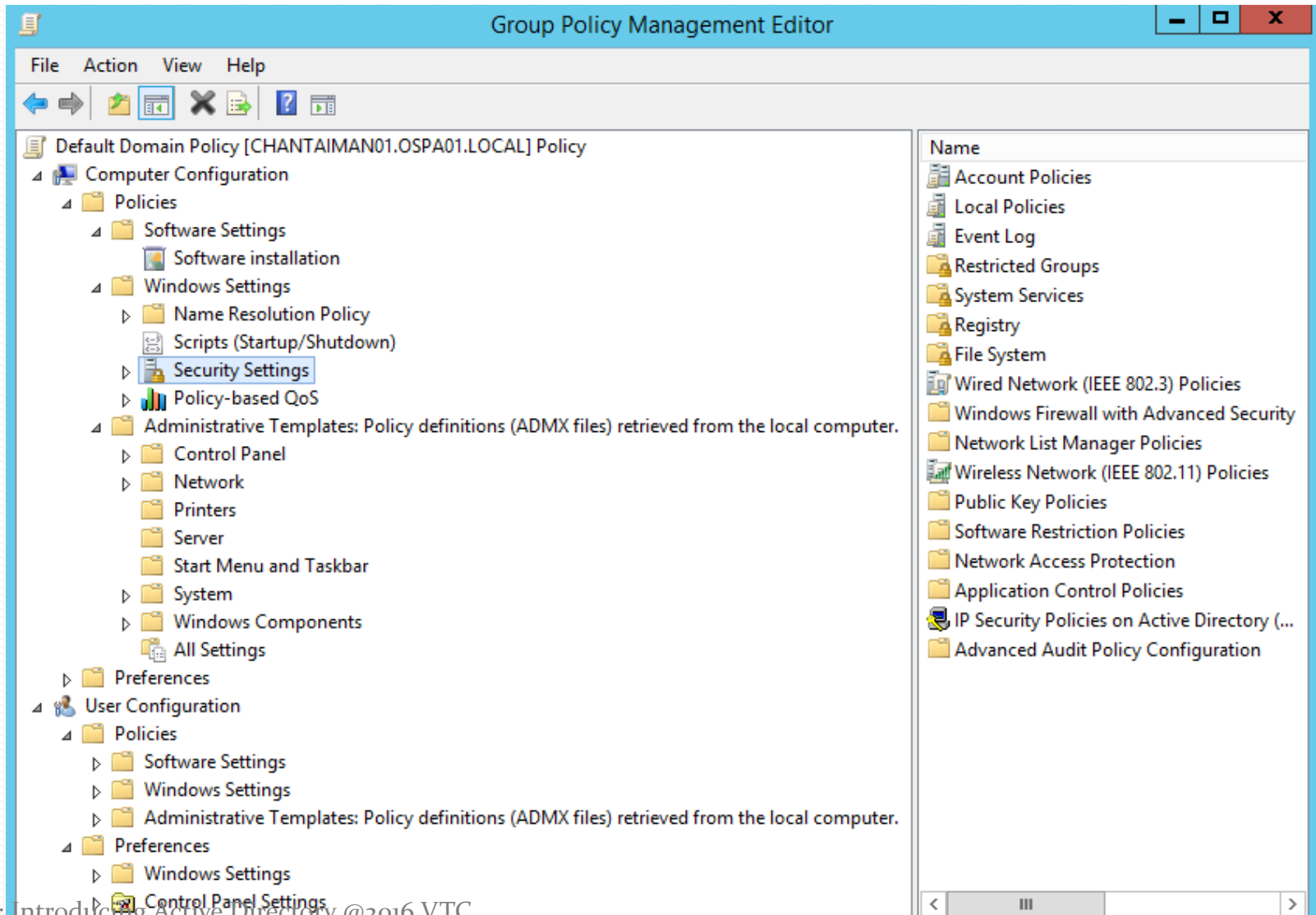
1. Computer Configuration

- Used to set policies that **apply to computers** within the GPO's scope
 - affect the computer environment by *implementing changes in the OS settings, hardware settings, applications, etc.*

2. User Configuration

- Used to set policies that **apply to all users** within the GPO's scope
 - affect the user environment including *desktop appearance, available applications, start menu, etc.*

Group Policy Management Editor



1. Computer Configuration Node

❖ THREE default policy subnodes

- Software Settings
 - Enable administrators to **install and manage applications remotely**
- Windows Settings
 - Set policies for folder redirection, scripts, and security
 - Contain *Name Resolution Policy folder and Scripts (Startup/Shutdown), Security Settings, and Policy-based QoS nodes*
- Administrative Templates
 - Set policies for OS, Windows components, and programs
 - Contain *Control Panel, Network, Printers, Server, Start Menu and Taskbar, System, and Windows Components folders*

2. User Configuration Node

- ❖ Contains the same THREE policy folders as in the Computer Configuration node BUT **policies defined here affect domain users within the GPO's scope, regardless of which computer the user logs on to**
 - Software Settings
 - Contain *Software installation node*
 - Windows Settings
 - Contain *Scripts (Logon/Logoff), Security Settings, Folder Redirection and Policy-based QoS nodes*
 - Administrative templates
 - Contain *Control Panel, Desktop, Network, Shared Folders, Start Menu and Taskbar, System, and Windows Components folders*

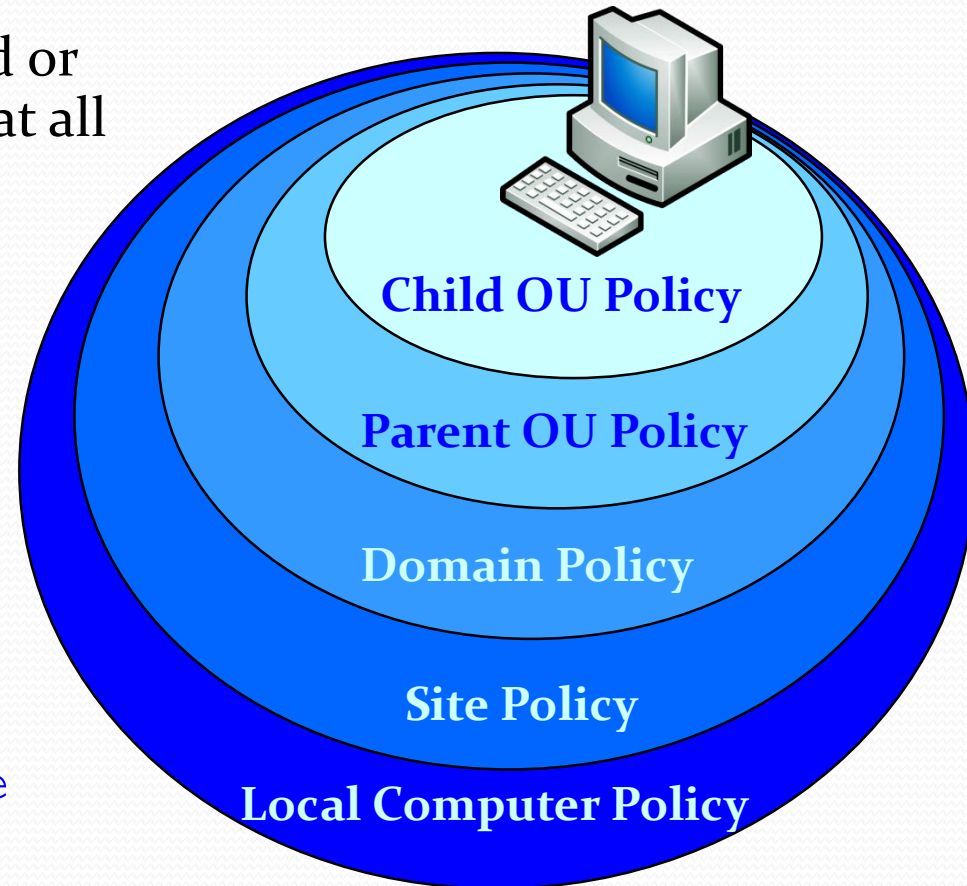
How Group Policies are Applied?

❖ Application order

- Local → Site → Domain → Organizational Units
 - Policies that are not defined or configured are not applied at all
 - Last policy to be applied takes precedence

❖ When?

- Startup and shutdown
- Logon and logoff
- Defined time intervals
- Forced with `GPUpdate.exe`



Summary

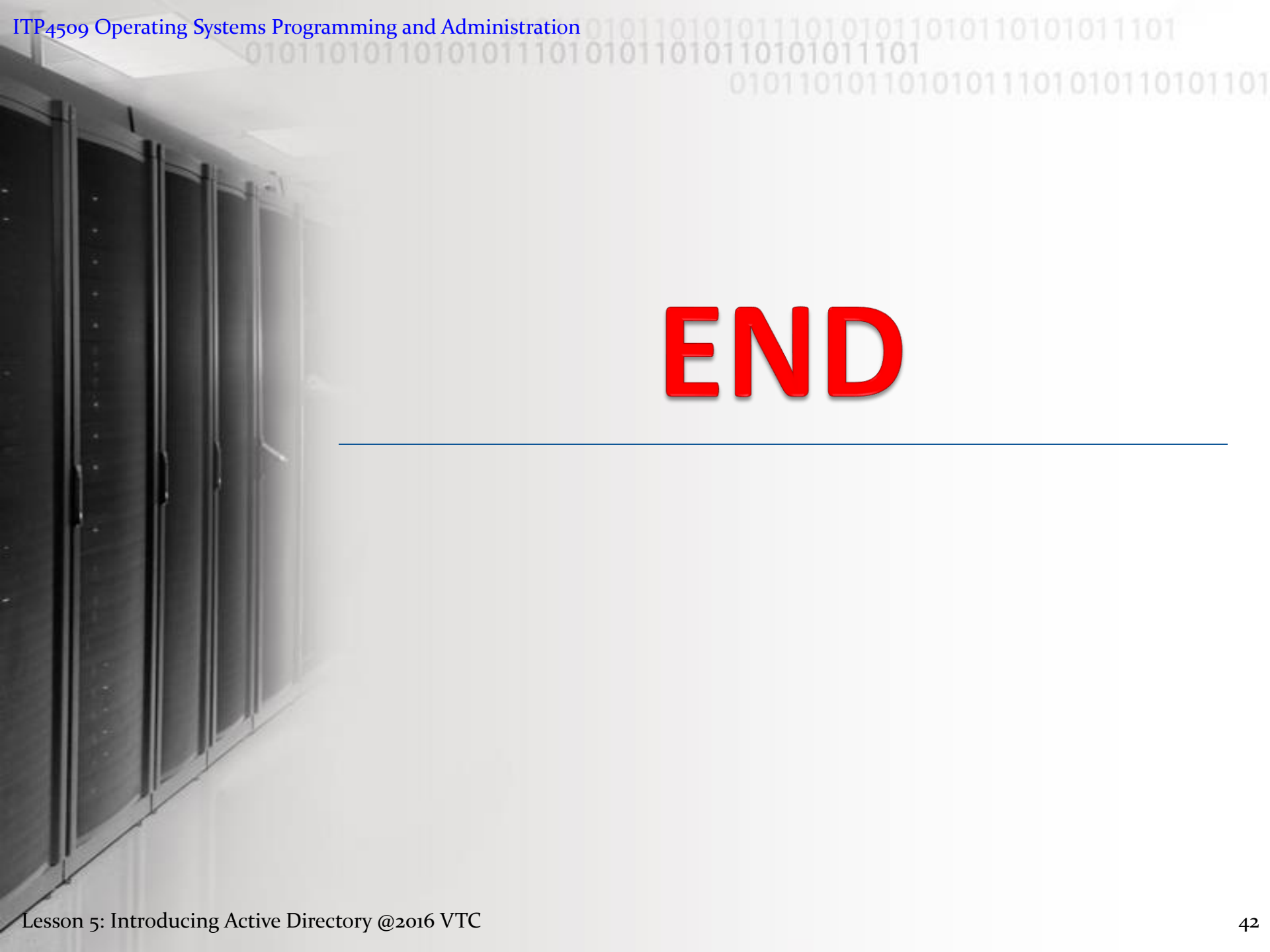
- ❖ A Directory Service is a DB that stores network resources information and can be used to manage users, computers, and resources throughout the network
- ❖ **A**ctive **D**irectory is a hierarchical, distributed DB that's scalable, secure, and flexible
 - AD's physical structure is composed of **S**ites and **D**omain **C**ontrollers, and the logical structure is composed of **O**rganizational **U**nits, **D**omains, **T**rees, and **F**orests
- ❖ Server Manager installs the DNS Server and **A**ctive **D**irectory **D**omain **S**ervices role
 - Promote the server to a domain controller is required to finish installation

Summary (cont.)

- ❖ The data in AD is organized as **objects**
 - Available objects and their structure are defined by the AD **Schema**, which is composed of schema **classes** and schema **attributes**
 - The data in a schema attribute is called an attribute value
 - Two types of objects:
 - Container Objects and Leaf Objects
 - Leaf objects generally represent security accounts, network resources, and GPOs
- ❖ AD objects can be located easily with search functions in Active Directory Users and Computers and Windows Explorer

Summary (cont.)

- ❖ **GPOs** are lists of settings that enable administrators to configure user and computer operating environments remotely
 - Group Policy Management Console (GPMC) Snap-in
 - Policies defined in the **Computer Configuration** node affect all computers in the AD container to which the GPO is linked
 - Policies defined in the **User Configuration** node affect all users in the AD container to which the GPO is linked



END
