



Microsoft® **Windows®**

UBNetDef, Spring 2022

Week 4

Vasudev Baldwa

Learning Goals

- Understand the difference between Server Desktop and Server Core
- Identify the elements of an Active Directory system
- Create and configure group policy objects
- Distinguish between security groups and organizational units

Agenda

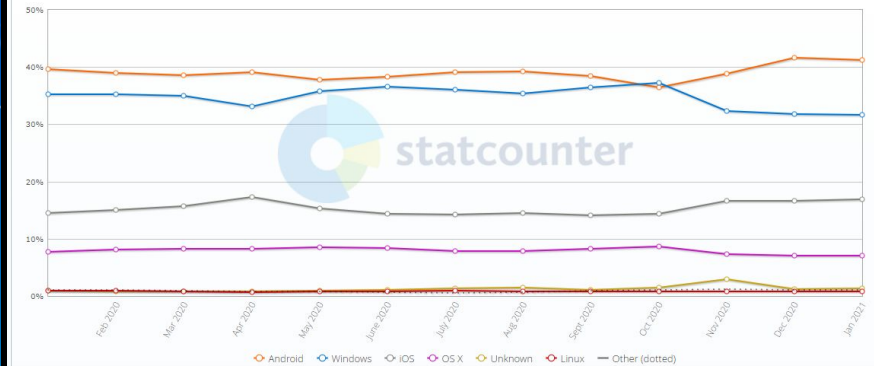
1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Windows Server vs Client

- Windows Client is the tried and true Windows OS that all of you are familiar with
- Windows Server is a OS designed to offer network based services on the Windows Platform

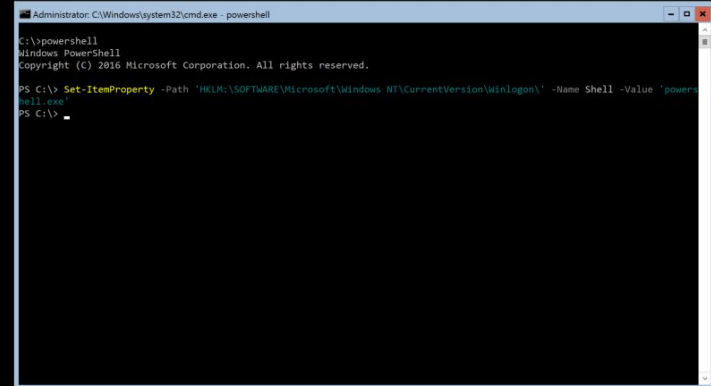
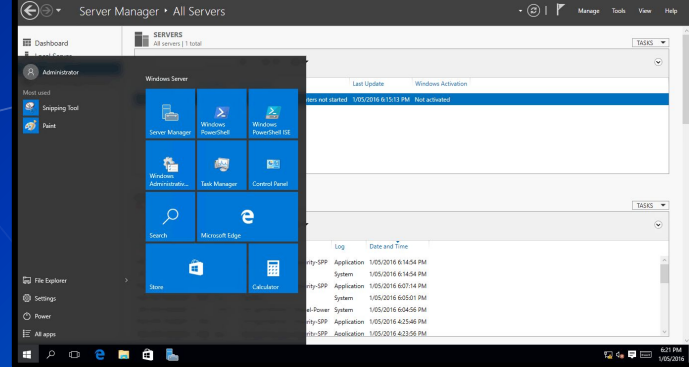


Operating System Market Share Worldwide
Jan 2020 - Jan 2021



Windows Server(s)

- Windows Server comes in 2 flavors
 - Server Desktop - Looks a lot like a Windows client
 - Server Core - Just a command line prompt
- Core and Desktop have the same functionality, but core is command based only.
 - Designed to be managed on a "headless system" or remotely



Windows System Level Authority

- Special type of account
 - pre-existing
- Local account (individual per machine)
- Used by the operating system to run Windows related programs
- **Has the highest privileges on the system**
 - User < Administrator < System

```
whoami      : nt authority\system
GetCurrent : NT AUTHORITY\SYSTEM
```


Command Lines

- PowerShell vs Command Prompt
- Command Prompt is based on MS-DOS
 - Outdated, usually avoid using
- Powershell
 - Newer CLI designed for server administration
 - Need to find the right commands.
 - Google and Microsoft documentation are your friends
 - Many commands are in the Verb-Noun format
 - Get-WebContent, ForEach-Object etc.

```
Microsoft Windows [Version 10.0.18362.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\anthony>help
For more information on a specific command, type HELP command-name
ASSOC      Displays or modifies file extension associations.
ATTRIB     Displays or changes file attributes.
BREAK      Sets or clears extended CTRL+C checking.
BCDEDIT    Sets properties in boot database to control boot loading.
CACLS      Displays or modifies access control lists (ACLs) of files.
CALL       Calls one batch program from another.
CD          Displays the name of or changes the current directory.
CHCP       Displays or sets the active code page number.
CHDIR      Displays the name of or changes the current directory.
CHKDSK     Checks a disk and displays a status report.
CHKNTFS    Displays or modifies the checking of disk at boot time.
CLS        Clears the screen.
CMD        Starts a new instance of the Windows command interpreter.
COLOR      Sets the default console foreground and background colors.
COMP       Compares the contents of two files or sets of files.
COMPACT    Displays or alters the compression of files on NTFS partitions.
CONVERT    Converts FAT volumes to NTFS. You cannot convert the
           current drive.
COPY       Copies one or more files to another location.
DATE       Displays or sets the date.
DEL        Deletes one or more files.
DIR        Displays a list of files and subdirectories in a directory.
DISKPART   Displays or configures Disk Partition properties.
DOSKEY     Edits command lines, recalls Windows commands, and
           creates macros.
```

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.
```

```
https://aka.ms/powershell
Type 'help' to get help.
```

```
A new PowerShell stable release is available: v7.1.4
Upgrade now, or check out the release page at:
https://aka.ms/PowerShell-Release?tag=v7.1.4
```

```
PS /home/sysadmin> whoami
sysadmin
PS /home/sysadmin>
```

Agenda

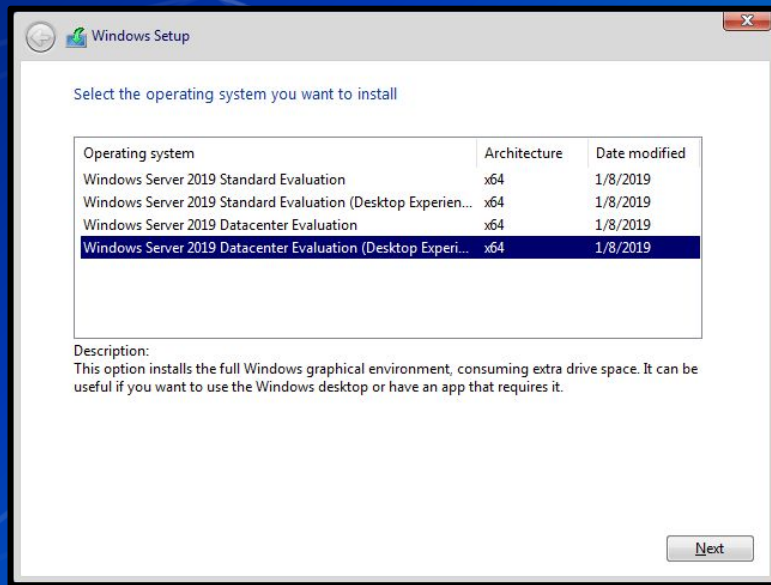
1. Windows Systems Information
2. Install Server Desktop Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Hands On

Install Server Desktop Experience on your AD machine

Hands-on: Start Windows Install

- Start the install for Windows Server 2019 Evaluation
 - Mount the ISO `WindowsServer2019Eval.iso`
 - Install **Windows Server (Desktop Experience)** for your Active Directory Server



Agenda

1. Windows Systems Information
2. Install Server Experience
3. **Services**
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Services And Processes

- Services and Processes

- Common processes are instances of a program
 - notepad.exe, mspaint.exe, Rocket League
 - Often initiated and terminated by user action
- Active services are persistent processes
 - Xbox Live Game Service, Windows Update manager
 - Often run in the background
- Services are known to the OS whether they are running or not

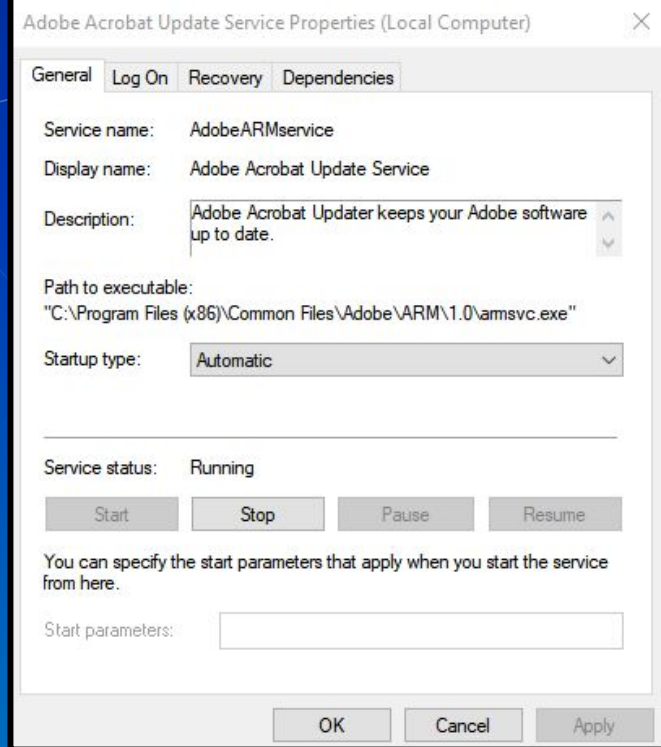
- Typically manage things that make the system work

```
PS C:\WINDOWS\system32> get-service
```

Status	Name	DisplayName
Stopped	AarSvc_517345d	Agent Activation Runtime_517345d
Running	AdobeARMservice	Adobe Acrobat Update Service
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	aspnet_state	ASP.NET State Service
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AtherosSvc	AtherosSvc
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	AudioSrv	Windows Audio
Stopped	autotimesvc	Cellular Time
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserSer...	GameDVR and Broadcast User Service
Stopped	eneSvc	BitLocker Drive Encryption Service

Services

- Services in Windows have a trait called a “start-up type”
 - Automatic
 - Starts automatically (on system boot)
 - Automatic Delayed Start
 - Starts after a set amount of time
 - Manual
 - Needs to be manually started
 - Disabled
 - Service won't start unless re-enabled



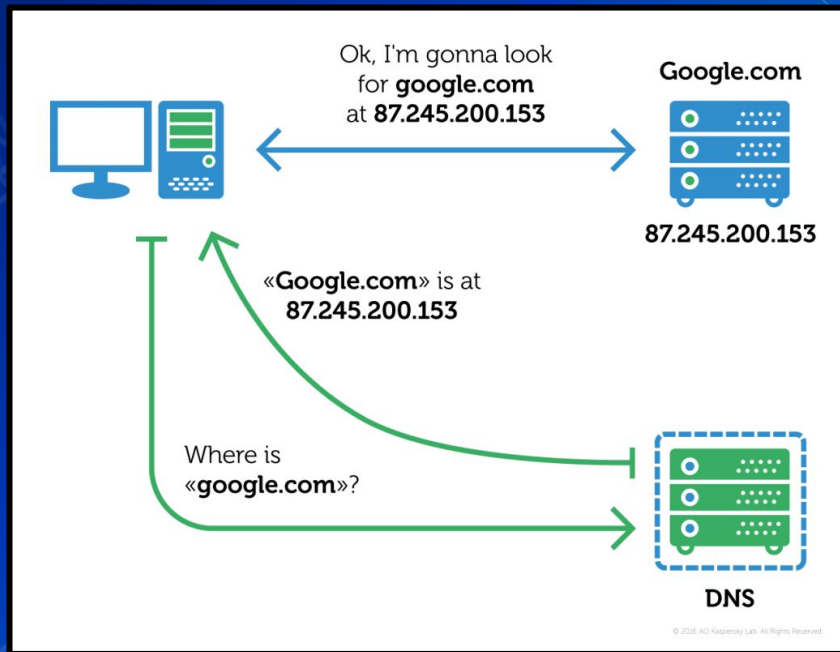
```
PS C:\WINDOWS\system32> Restart-Service Spooler -v
VERBOSE: Performing the operation "Restart-Service" on target "Print Spooler (Spooler)".
```


Windows Server Services

- Windows Server can provide a lot of services
 - Web Server
 - Internet Information Service (IIS)
 - File Share Services
 - Server Message Block (SMB)
 - Network file share / shared drive
 - Network Management Services
 - Domain Name System (DNS)
 - Dynamic Host Configuration Protocol (DHCP)

DNS

- Domain Name Services (DNS) translates URLs to IP addresses



Windows Server Services

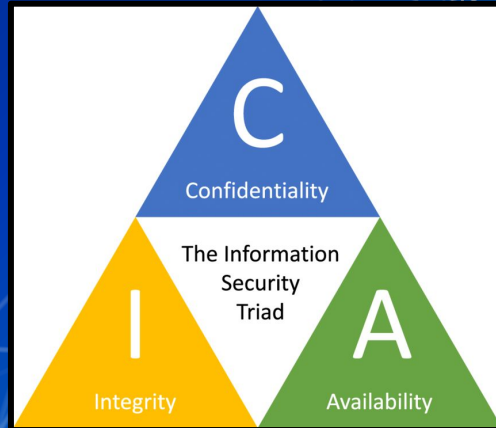
- Windows Server can provide a lot of services
 - Active Directory -> Identity and Access Management (IAM) Service
 - Usually what people use Windows Server for.
 - We use it at UB (@buffalo.edu)
 - Try to login to a computer

Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

IAM

- Authentication vs. Authorization
 - Verifying users' identity (authentication)
 - Granting them access to data based on their identity (authorization)
- IAM and the Confidentiality, Integrity, and Availability (CIA) triad
 - Which of the 3 pillars of the CIA triad does IAM support?



IAM

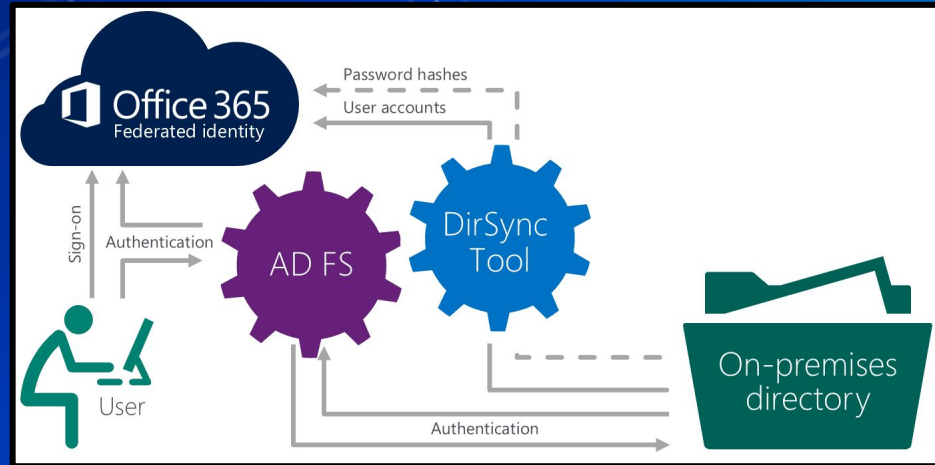
- Part of the Zero Trust Security Philosophy
 - Never trust that a user is who they say they are
 - Always verify the user's identity and level of access
- Multi-Factor Authentication (MFA) components:
 - Something the user knows
 - Something the user has
 - Something the user is
- Case in point: vCenter, UBLearns

IAM

- Part of the Zero Trust Security Philosophy
 - Never trust that a user is who they say they are
 - Always verify the user's identity and level of access
- Multi-Factor Authentication (MFA) components:
 - Something the user knows
 - Password
 - Something the user has
 - Duo, Secondary device
 - Something the user is
 - Biometrics (Fingerprint)
 - Less commonly used
- Case in point: vCenter, UBLearns

How does this work with AD?

- AD is primarily an IAM system
 - AD grants permissions to groups of objects
- Objects are users, computers, files, anything networked
- AD controls access to each object based on user authorization



QUESTIONS?

IAM can be complicated, but powerful.

Agenda

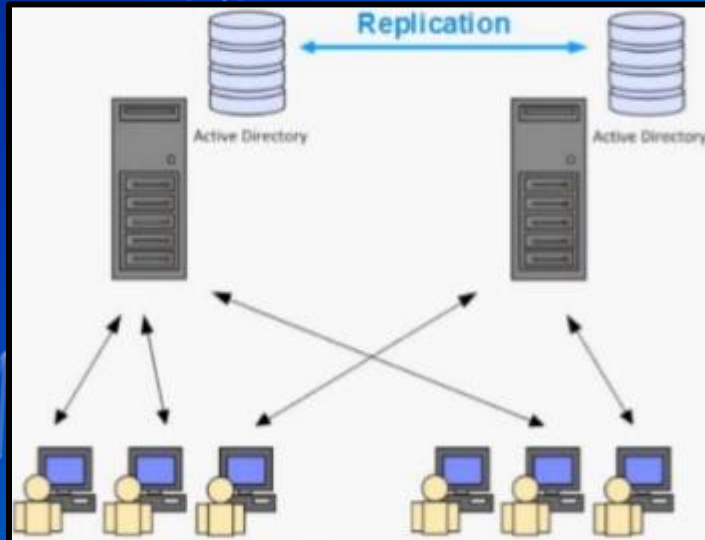
1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Components of an AD System

- Database of objects in a network (Domain)
 - Users
 - Computers
 - Printers
 - Security Groups
 - More
- The database is hosted on a Windows Server (called the Domain Controller)
 - Stores objects in hierarchy
 - Called organizational units (OU)
 - Can be based on real world hierarchy of organization
 - Can be based on access rights

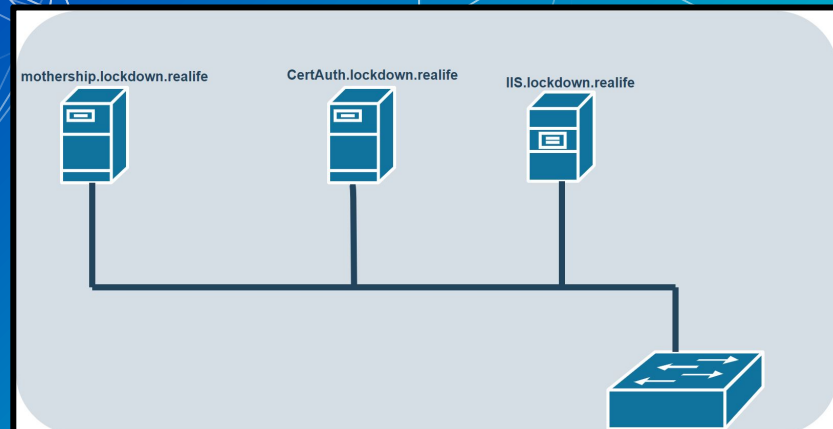
Domain Controllers (DC)

- Actually runs the AD Service (The Domain)
- Handles authentication requests for the domain
 - Also runs the DNS
- Can have multiple DCs to have redundancy or server load balancing



AD <3 DNS

- AD absolutely requires DNS to function
 - AD communicates with computers over domain names, not IP addresses
 - IPs can change
 - Computer names are unique per domain
- Your domain controller (that runs AD) also usually* serves as the local AD DNS server



Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. **Install AD Service**
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Hands On

Follow along with the me, directions are in mattermost if
you get lost

Break

10 mins

Hands On

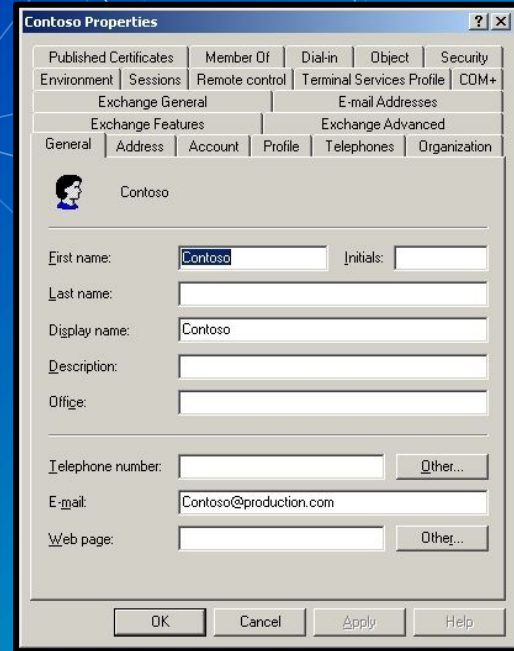
Follow along with the me, directions are in mattermost if
you get lost

Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Active Directory - User Objects

- What people authenticate against when they sign on
- Stores information on user
 - **Username**
 - Display name
 - Email
 - Phone number
 - Address
 - Location in organization
 - **Password (hashed)**



The screenshot shows the 'Contoso Properties' dialog box with the 'General' tab selected. The dialog box contains the following fields and options:

- First name:** Contoso
- Initials:** (empty)
- Last name:** (empty)
- Display name:** Contoso
- Description:** (empty)
- Office:** (empty)
- Telephone number:** (empty) with an 'Other...' button
- E-mail:** Contoso@production.com
- Web page:** (empty) with an 'Other...' button

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

Active Directory - User Objects

- AD controls permissions
 - File and folder access
 - VPN access
 - Password management
 - Active account
 - Access control
 - Ability to control total network access
- Map drives to computer (Network drives)
 - UB uses this as well. Log into a ub computer. You'll see an S: drive.
- Folder redirection

Administrator Properties

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

User logon name:

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:

My Company



Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

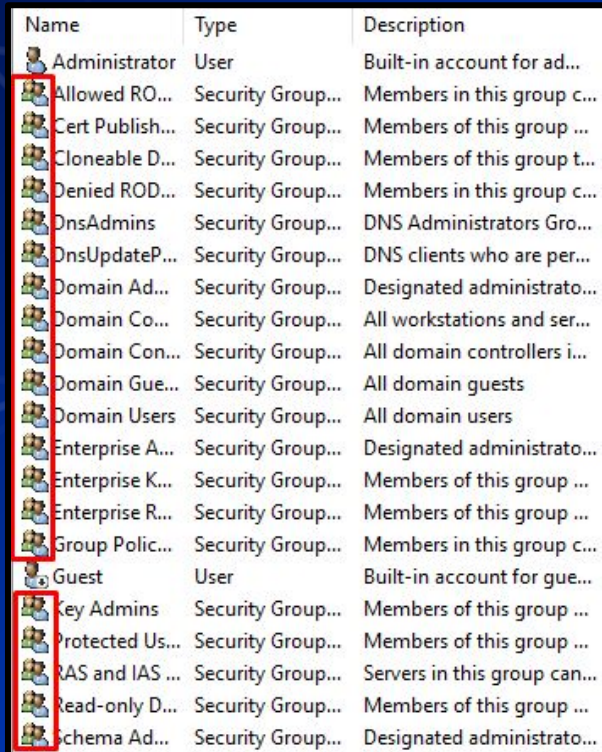
Active Directory - Security Groups

- We need a new object for each user. -> Too many to safely manage
 - UB has about 50,000 users on its main domain
- Security issues:
 - What happens when someone leaves?
 - What happens when we need to change permissions on every single student (~30K)
- Use Groups instead!

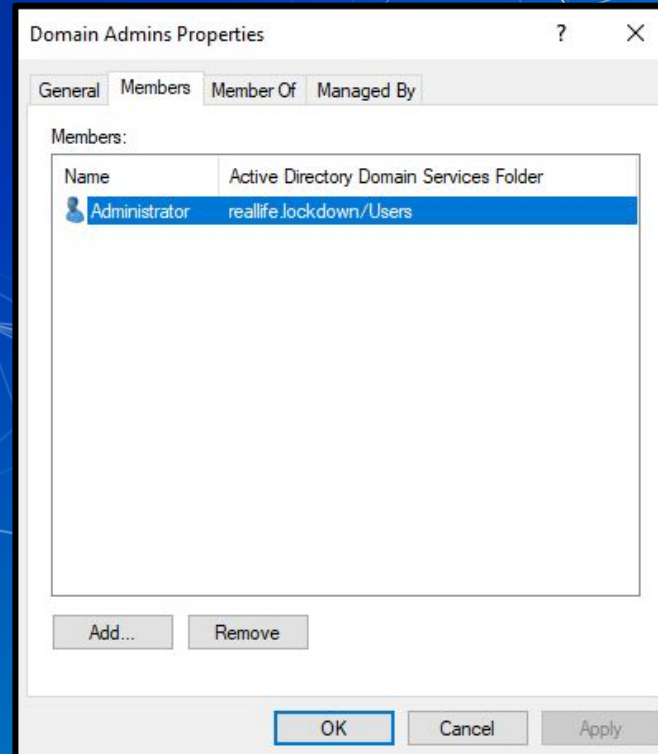
Active Directory - Security Groups

- Groups are a special "folder"
 - Objects can be put in groups
 - Helps keep organized
 - Can assign settings to groups
 - Acts similarly to users configuration
 - Manage every user at once that in the group

Active Directory - Security Groups



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...



My Company



```
graph TD; MC[My Company] --- S[Supporter]; MC --- B[ ]; B --- F[Finance]; B --- M[Marketing]; F --- F1[ ]; F --- F2[ ]; M --- M1[ ]; M --- M2[ ]; F1 --- I1[ ]; F2 --- I2[ ]; M1 --- I3[ ]; M2 --- I4[ ]; I4 --- I4Info[Name: John Doe<br/>Email: john@company.com<br/>Department: Marketing<br/>Phone: -123<br/>Title: Technical Writer];
```

The diagram is an organizational chart for 'My Company'. At the top is a blue box labeled 'My Company'. A line descends from it and splits into two branches. The left branch leads to a blue box labeled 'Supporter'. The right branch leads to a large, empty blue rectangular area. From the 'Supporter' box, a line descends and splits into two branches leading to 'Finance' and 'Marketing' boxes. Below 'Finance' are two person icons. Below 'Marketing' are two person icons. A line connects the bottom-most icon (a man in a green shirt) to a white box containing contact information.

Supporter

Finance

Marketing

Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

My Company

Supporter

Finance

Marketing



Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Active Directory - Nesting

- Can put groups in groups
- **Starts to get real complicated real dang fast**
- Layout organization before building AD
 - Build domain based on network layout and permissions
 - Doesn't always look like your organization's hierarchy chart
 - Should the CEO have admin access? Why?
- Leads to group inheritance



Active Directory - Inheritance

- Think of trickle down theory, or Object Oriented Programming
- Sub groups (children objects) inherit permissions from group above (parent object)
- Users in a group, within another group, will get settings placed on top level group



Everyone can login

My Company

Only this group gets MS
Office access

Parent Group

Supporter

Child Groups

Finance

Marketing

User Objects

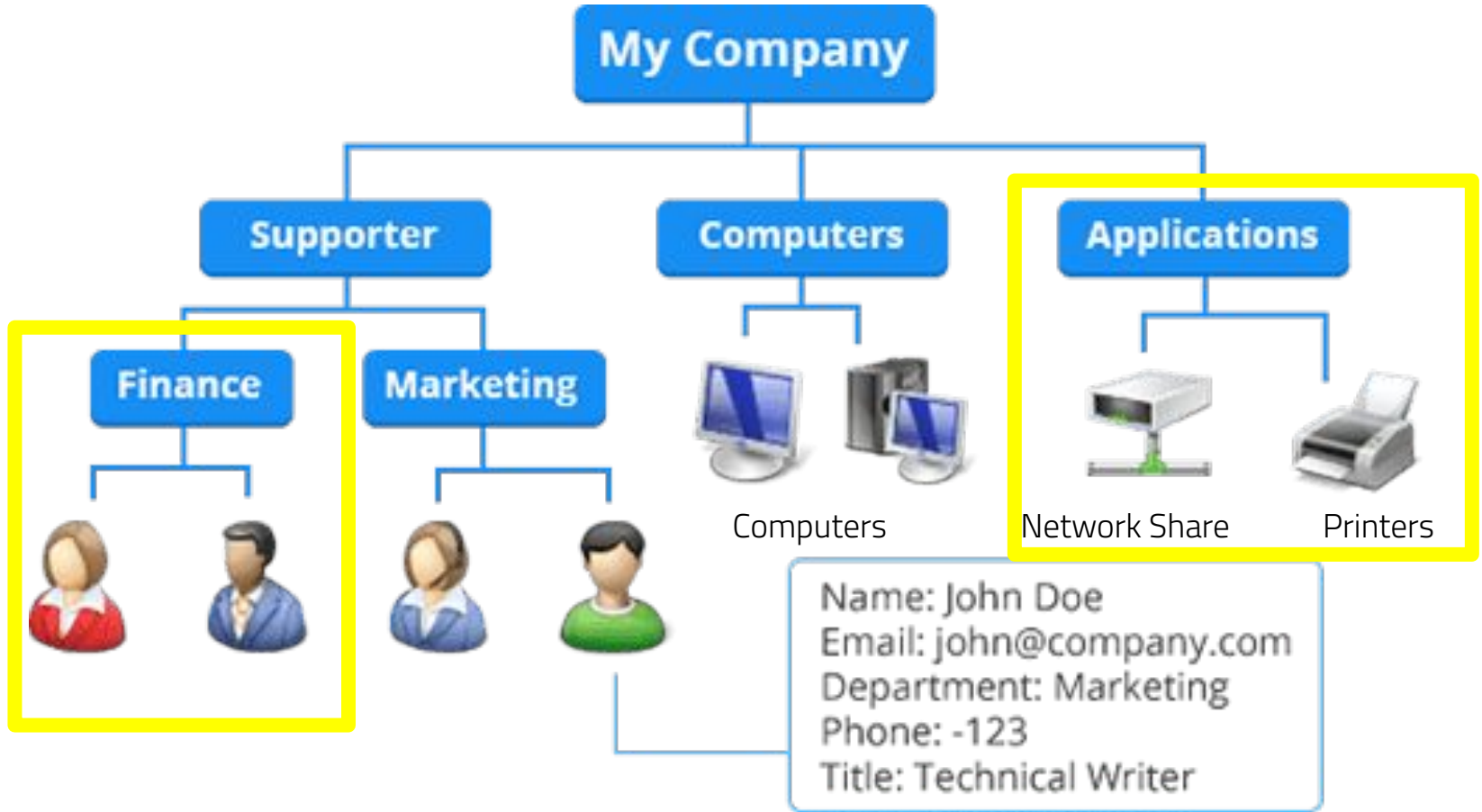


Only marketing can use
MS Paint.

Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Active Directory - Computers and Devices

- Like users, devices can also be managed by AD
 - E.g., computers, printers, other servers
- Control who gets to log-on
- AD allows for cross-device permissions
 - Have certain computers access certain printers



Active Directory - Introduction to OUs

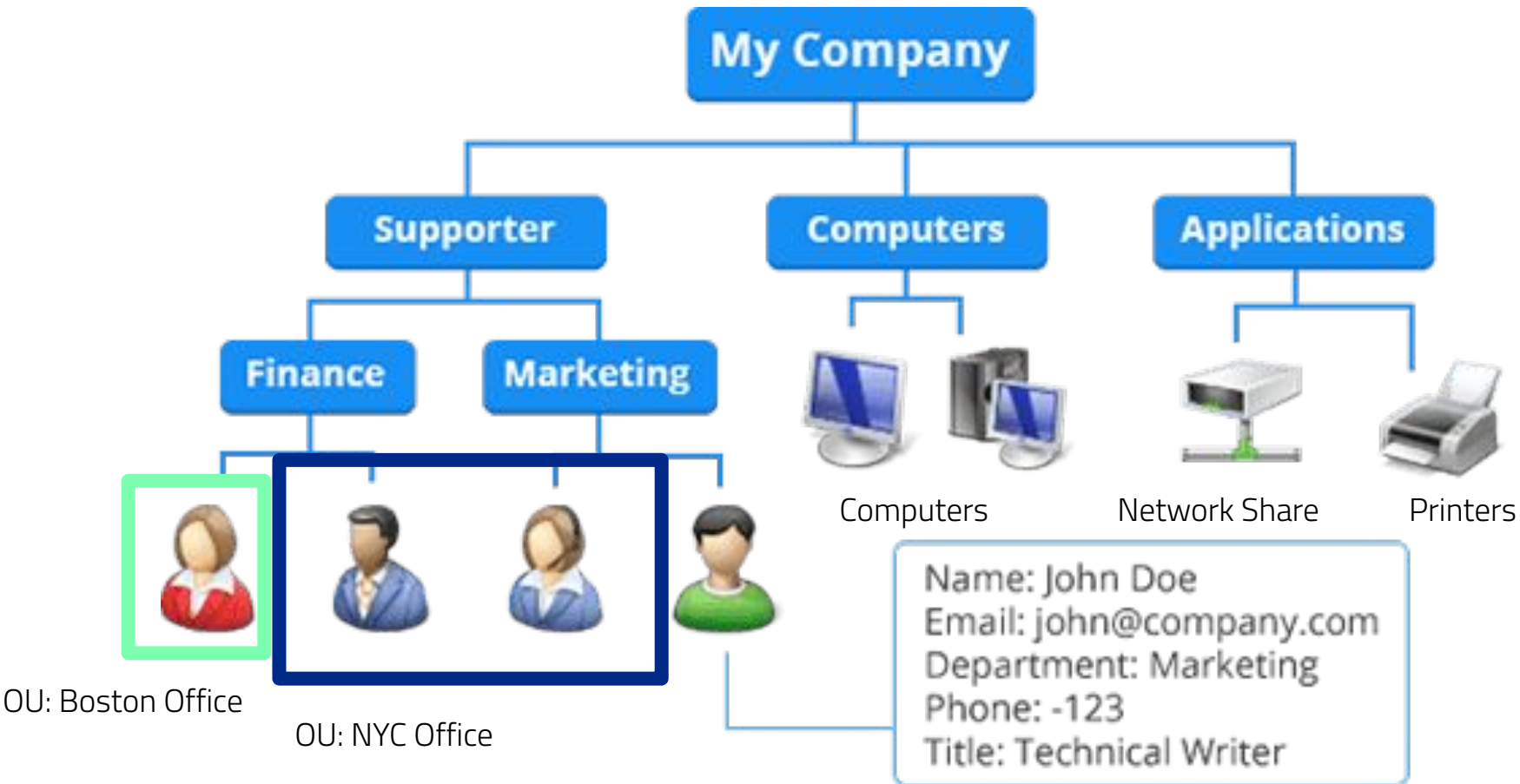
- All members of the student security group at UB can log into computers.
 - This is an IAM use case
- What if we want to group the students by degree program?
 - Is this an IAM use case?
 - When might it not be?

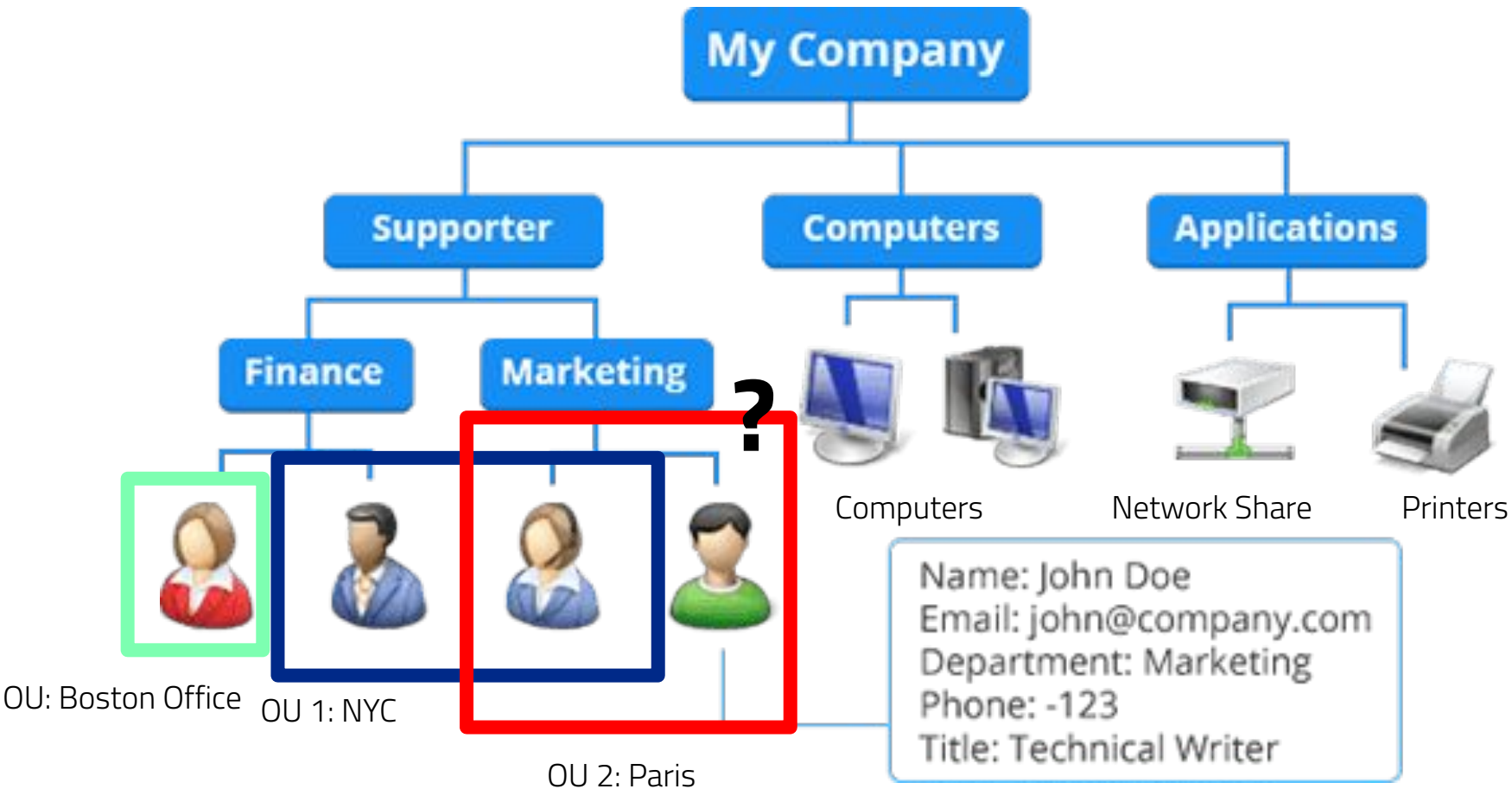
Active Directory - Introduction to OUs

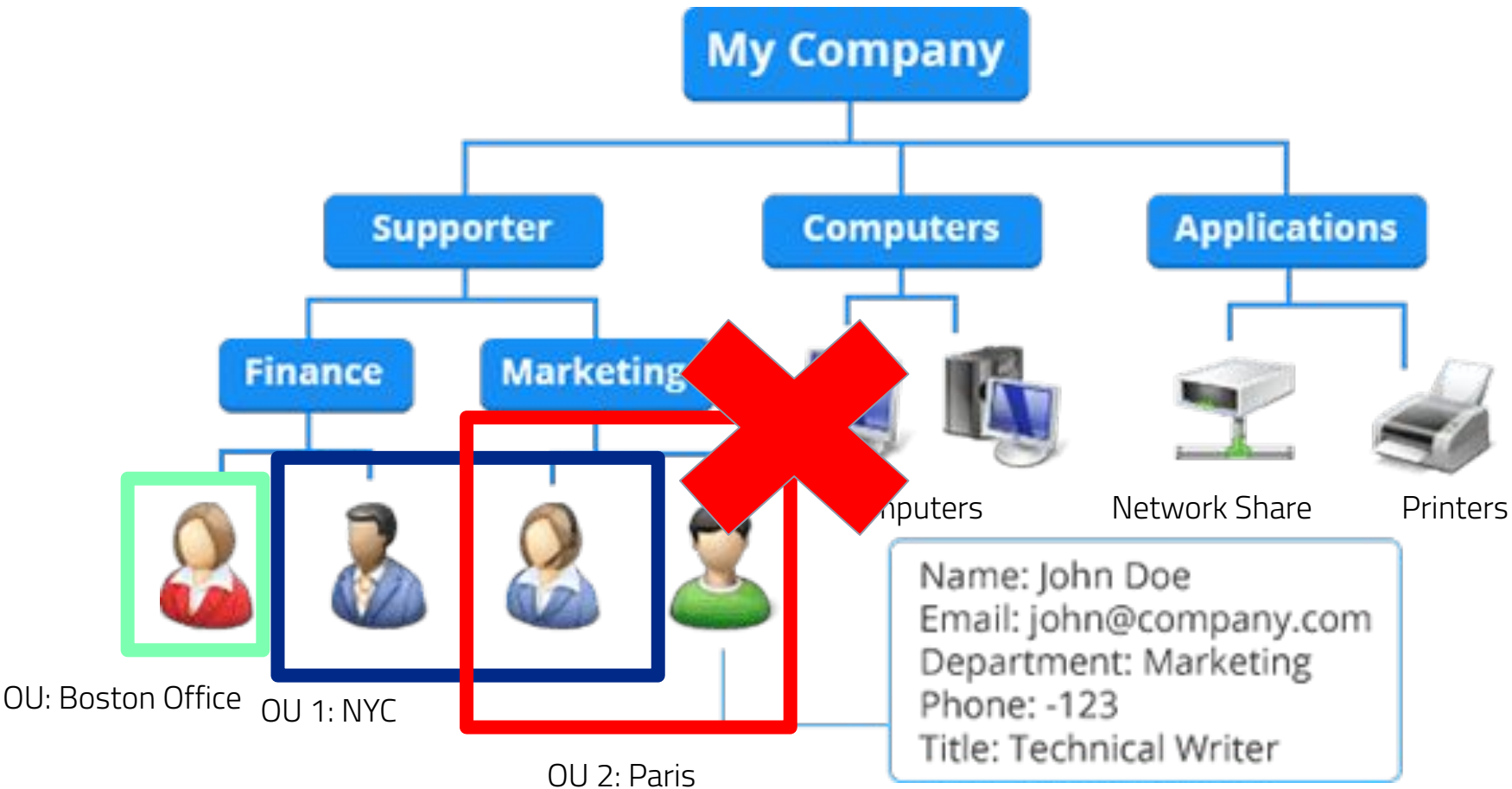
- We want the SEAS Students get a picture of Davis as their background.
- The SOM Students get a picture of Jacobs as their background.
- Are the backgrounds an IAM issue?
- How can we solve this problem?
 - What disadvantage is there to making multiple brand new security groups?

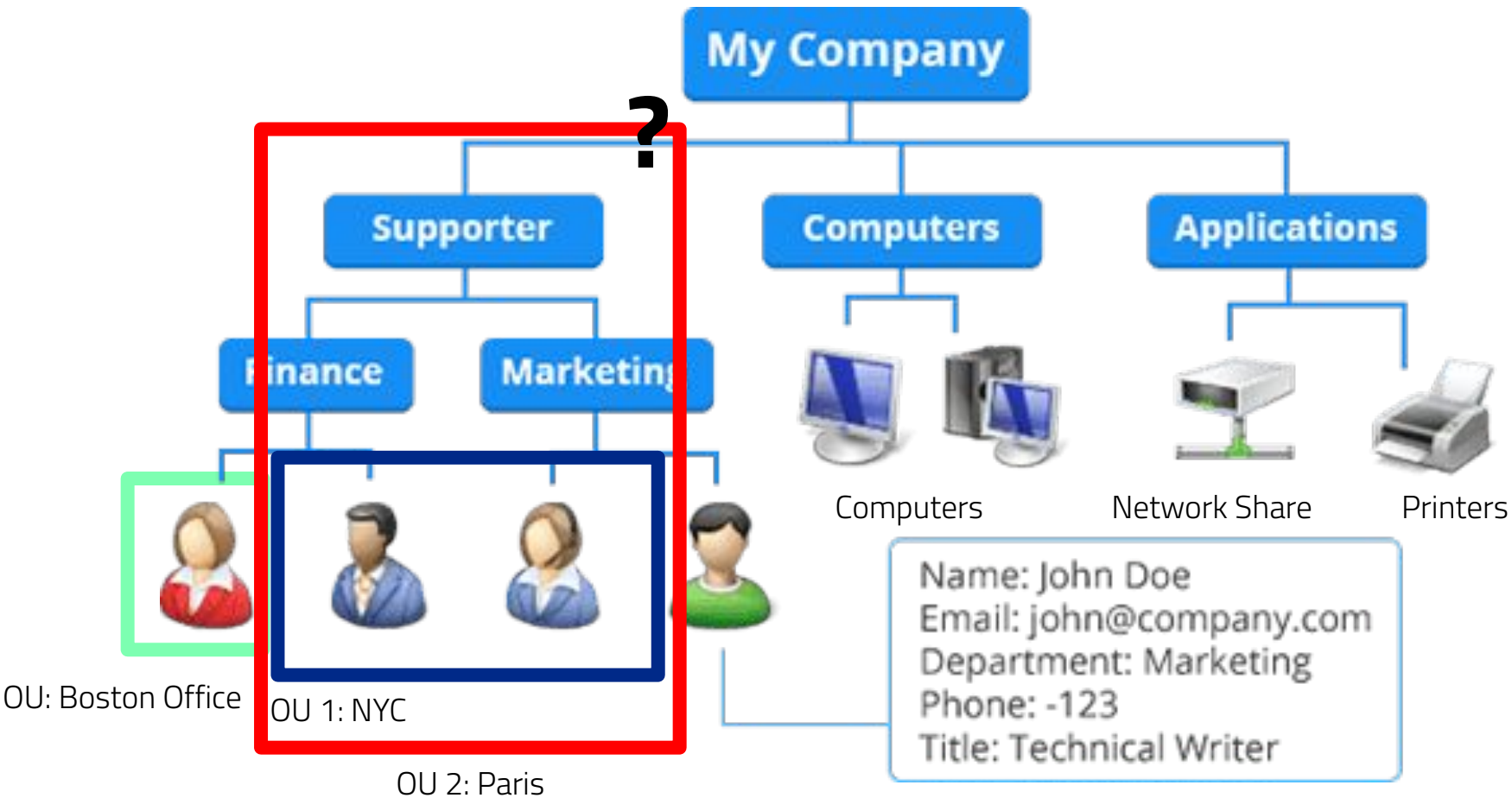
Active Directory - OUs

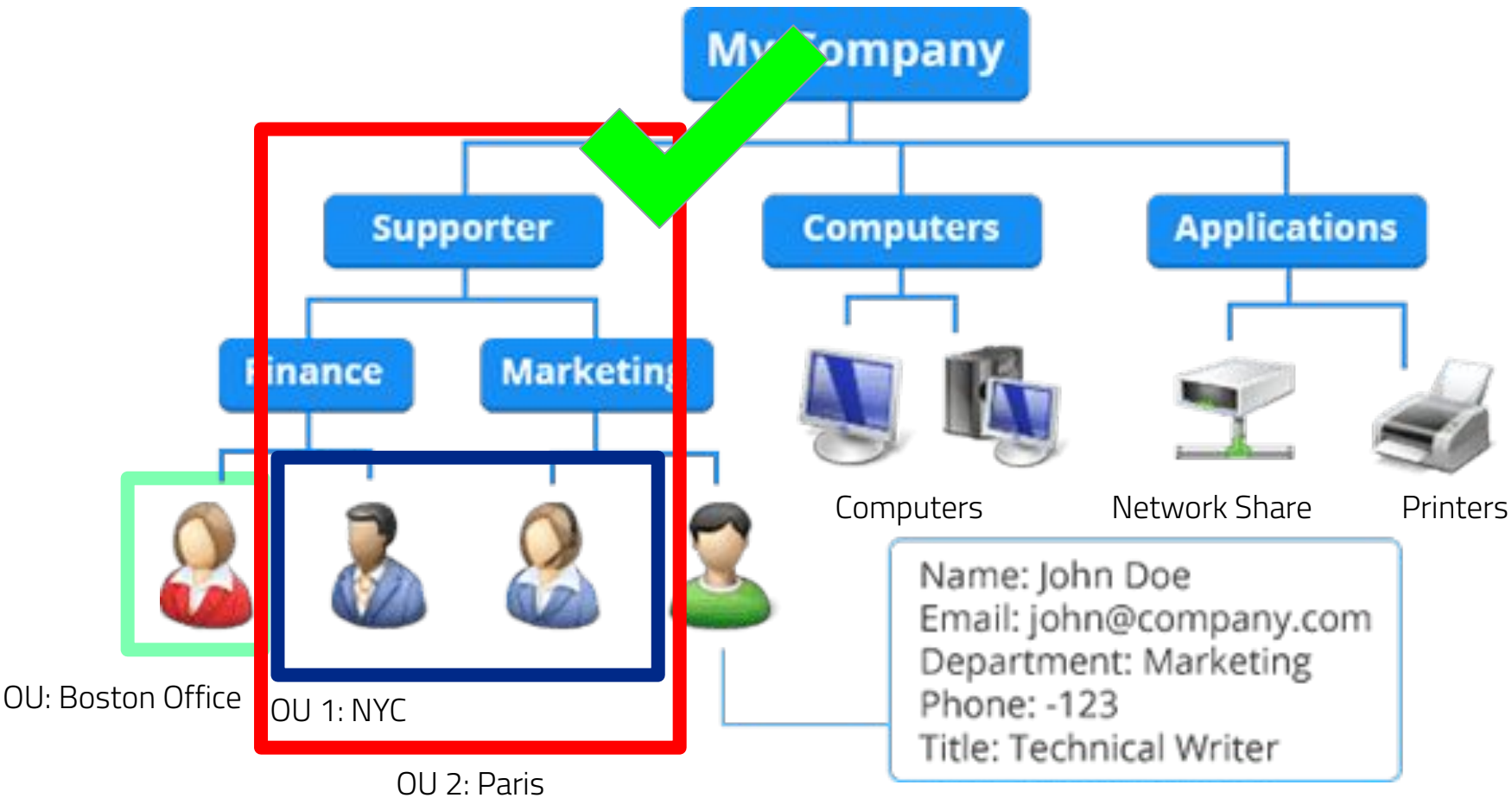
- Organizational Units (OU) are also used to collect objects together.
- **Differ from Security Groups**
 - Security Groups are necessarily IAM based
 - ALWAYS access based
 - Student vs Faculty
 - OUs are other ways to collect objects that are not IAM based
 - Often based on location, status (ex. Your major)
- **You can't be in more than one OU at the same level**
- OUs cannot be security-grouped together. They are not objects. They are not groups.





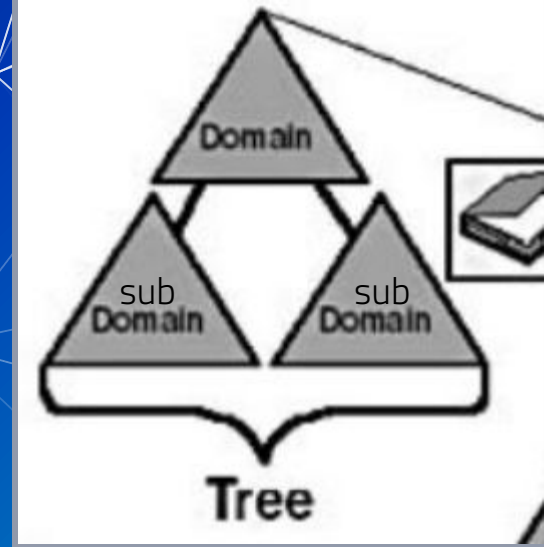






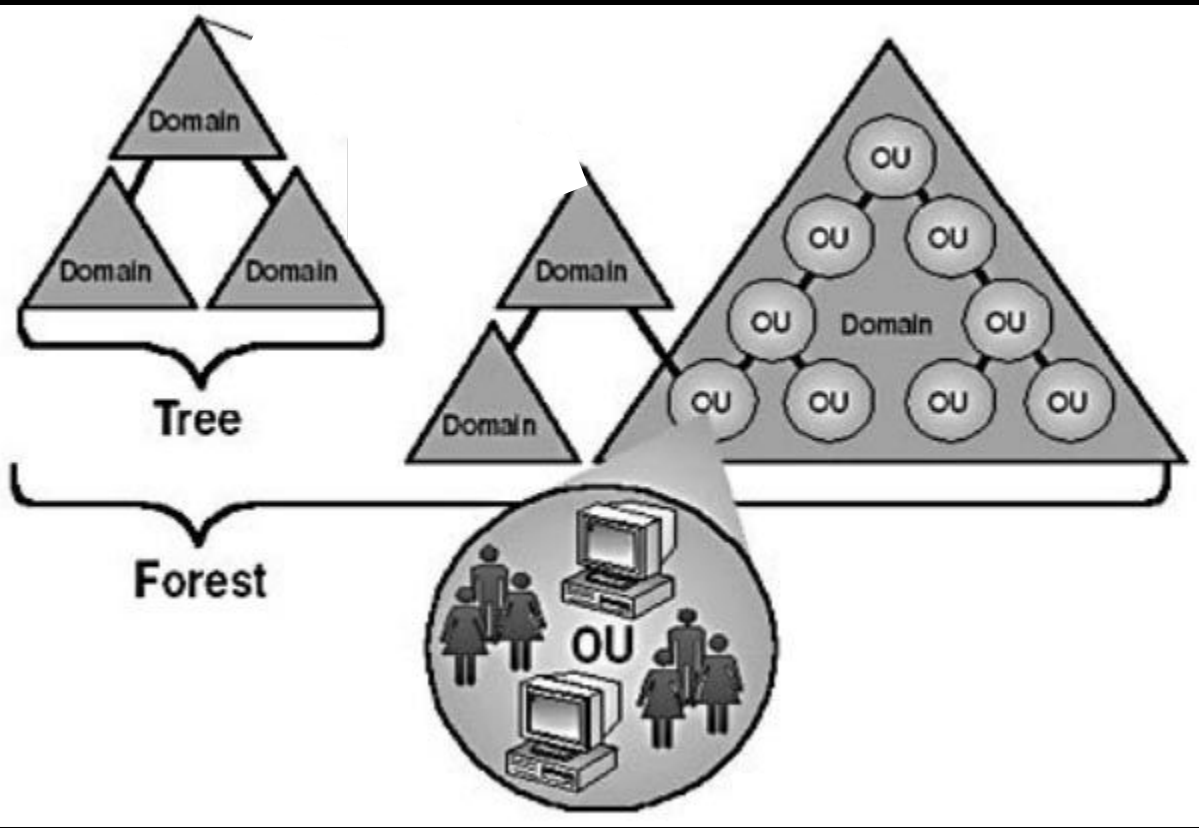
Active Directory - Trees

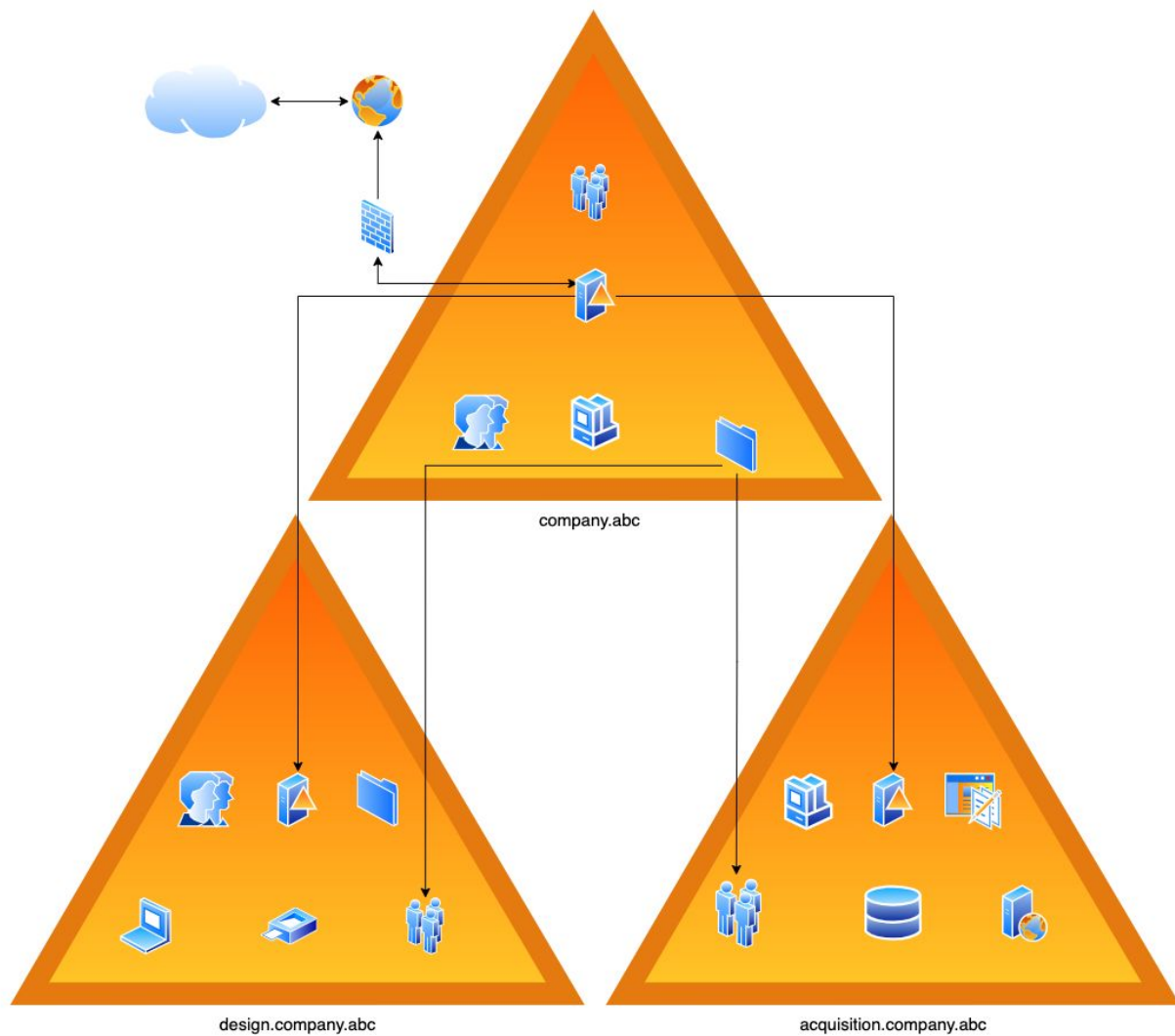
- Let's say we have a domain called company.xyz
 - company.xyz (domain) is composed of multiple objects
- company.xyz has 2 subdomains associated with it.
 - finance.company.xyz
 - marketing.company.xyz
- Each subdomain can be used to further **organize** the objects associated with company.xyz
- These subdomains and domain together are called an AD **Tree**
- We use trees to help with the logical management of the domain



Active Directory - Forests

- Let's say that Company ABC buys Company XYZ.
 - XYZ is now a subsidiary of ABC.
- Company ABC already has a domain set up. ABC can now manage the domains of ABC and XYZ together.
- Multiple Trees can be managed together
 - This hierarchy is called an AD **Forest**.
- A forest is a collection of one or more domain trees.
- As soon as you make a domain, you also have a tree (of 1 domain) and a forest of 1 tree





Confused? TL;DR for OUs

- Domains control networks
- Organizational Units (OU's) are collections of things (Objects)
- Groups also contain objects
- Groups can go in groups
- Children objects inherit permissions from parent objects
- Everything is inherited top to bottom

QUESTIONS?

Too many acronyms.

Break

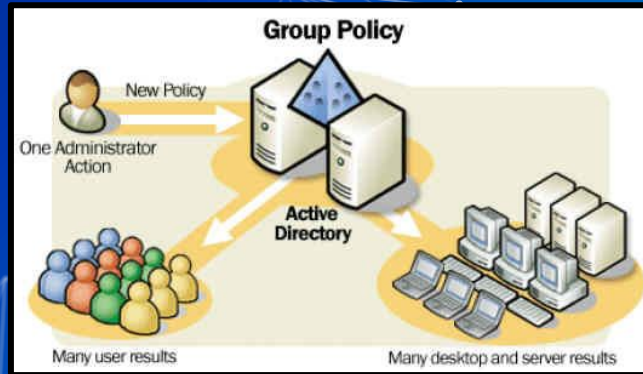
Please return in 10 mins

Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Active Directory - Group Policy Objects

- Group policies are settings that can be enforced on an entire domain
- Example: We want all desktops to have a certain background.
- Enforced in a hierarchical top down format from the domain level to the object level
 - If a higher policy exists, the higher policy is enforced



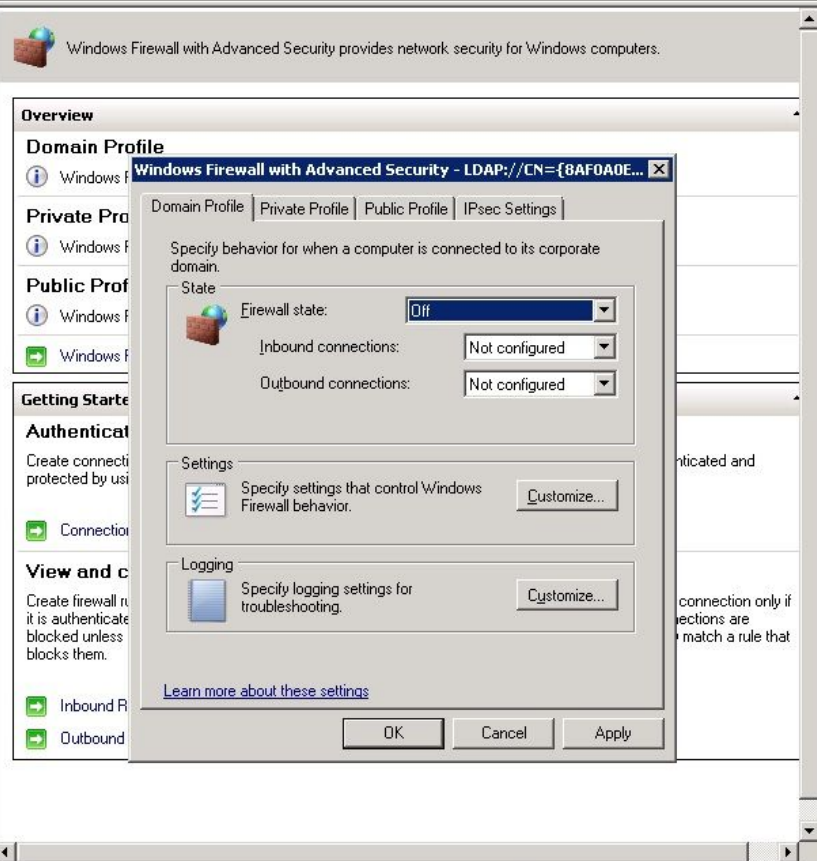
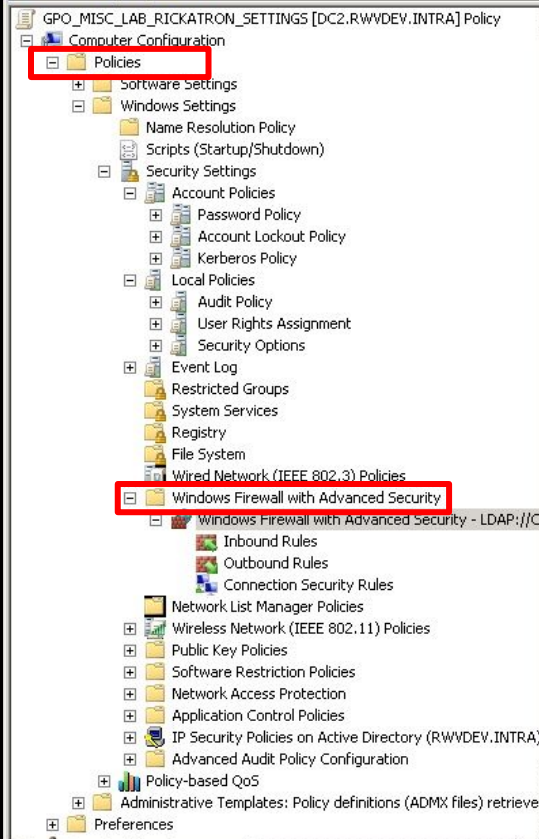
Group Policy Key Terms

- Enforced
 - Can not be overwritten by other policy
- Linked
 - Link policy to specific OU
- Filtering
 - Can choose to apply Group policy to objects that meet criteria
 - < 8GB RAM
- Group Policy Object (GPO)
 - A set of rules that can be applied to any object

Group Policy Examples

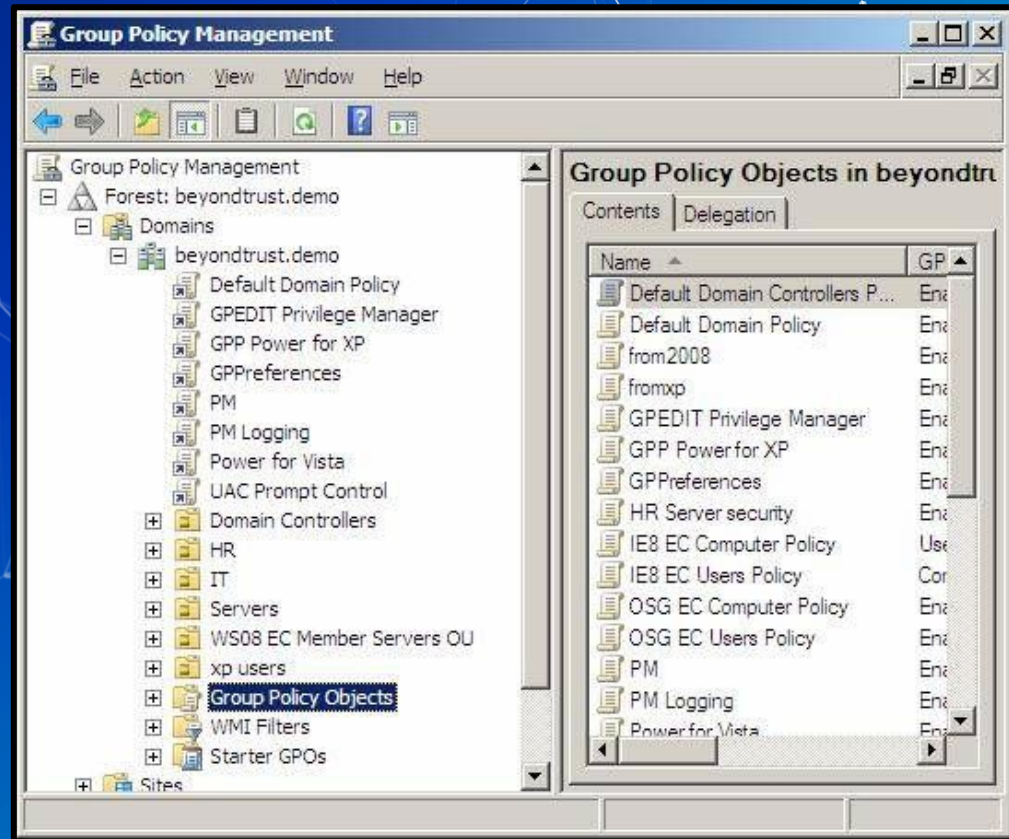
- Can be used to force any setting on objects/groups/OUs in AD
- Pretty much anything you can think of
- Security
 - Password policy
 - Powershell transcription
 - Set firewall policy
- Functional
 - Mapped network drives
 - Sleep settings
 - Remote desktop access
 - Windows Update timing
- Appearance
 - Change background
 - Change cursor





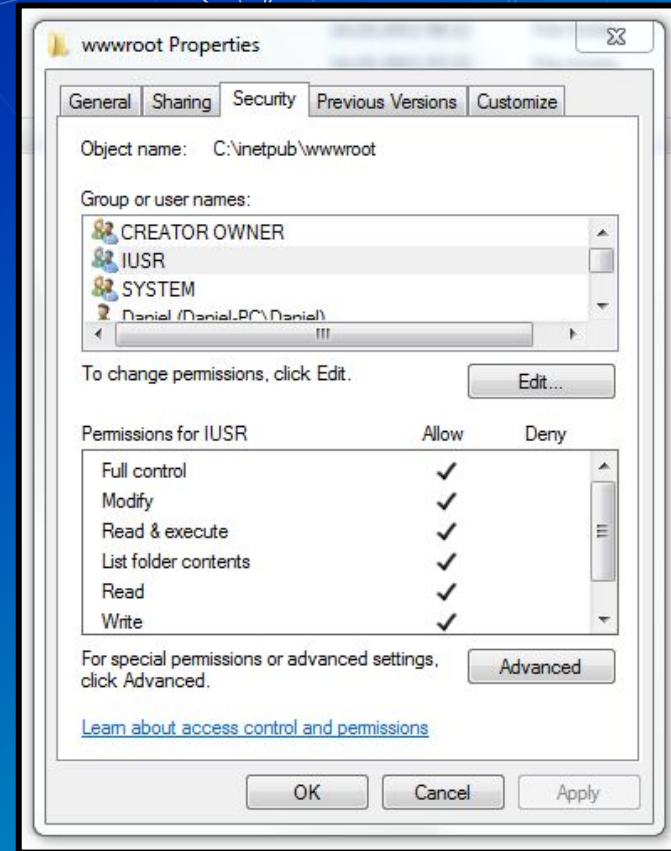
Multiple Group Policies

- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group
- **Group policies can be applied to any domain object**
 - Users, Computers, Groups



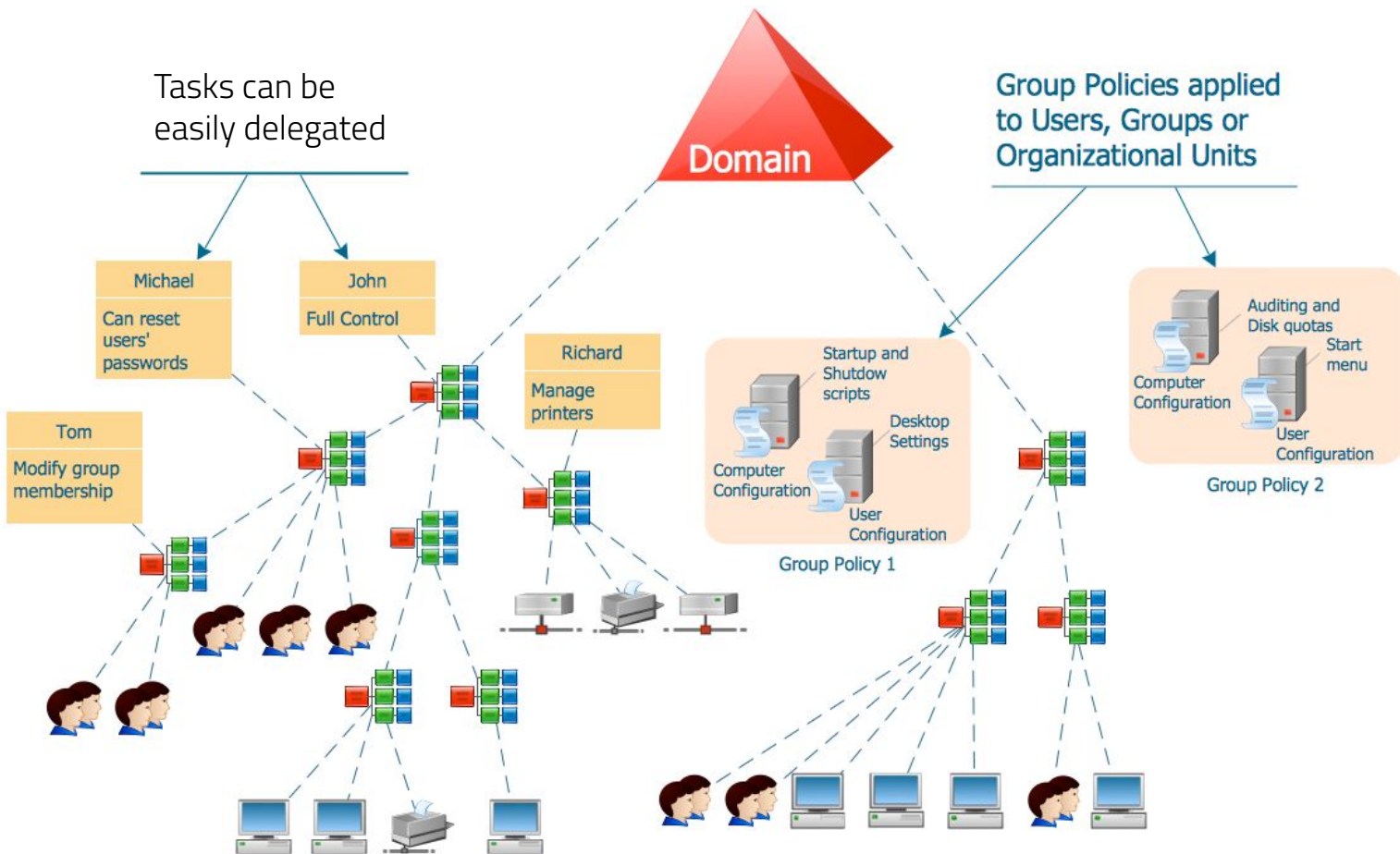
File Permissions

- Can be set on individual files, folders, network shares, hard drives
- Can specify who has read, write, or modify permissions
- File permissions can be inherited from containing folder
- Ex) Can share whole folder instead of every file
- Can be set using group policy and Active Directory









Tasks can be easily delegated

Group Policies applied to Users, Groups or Organizational Units



Legend

-  Organizational unit
-  Workstation
-  Group
-  Printer
-  Share
-  Policy

Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Powershell Execution Policies

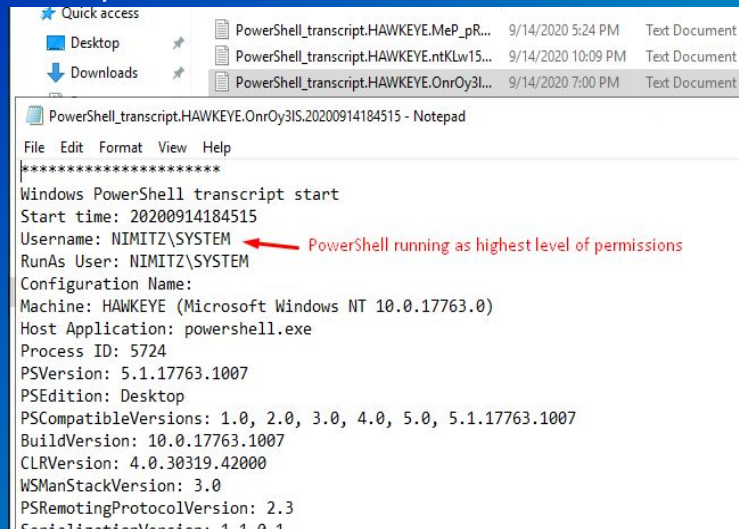
- Controls the conditions under which PowerShell loads configuration files and runs scripts.
 - Helps prevent execution of malicious scripts
- Not intended to be a security feature
 - Can help to mitigate your risk

```
PS /home/sysadmin> Set-ExecutionPolicy RemoteSigned
```


PowerShell Transcription

- Transcription is a method of logging PowerShell activity
- Why would we do this?
- Not enabled by default
 - Needs to be enabled by group policy

```
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="Attempted to perform an unauthorized operation."
New-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1
+ New-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Exc ... Windows protects Defender's registry keys
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (HKEY_LOCAL_MACHINE\Extensions:String) [New-ItemProperty],
UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.NewItemPropertyCommand
New-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1
```



Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
 - a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

Further Reading

[What is IAM?](#)

[MS Docs: Understanding AD](#)

[MS Docs: Powershell Reference](#)

Homework

Vasu will run OH on Tuesday 3/1 from 5:30 – 6:30 PM

And be present in Alec's OH on Thursday 3/3 from 5 – 6 PM

Summary and Wrap-up

Today's achievements:

- We identified the difference between Server Desktop and Server core
- We configured a domain controller
- We identified the differences elements of a domain system