UBNetDef, Fall 2021
Week 4
Vasudev Baldwa

Agenda

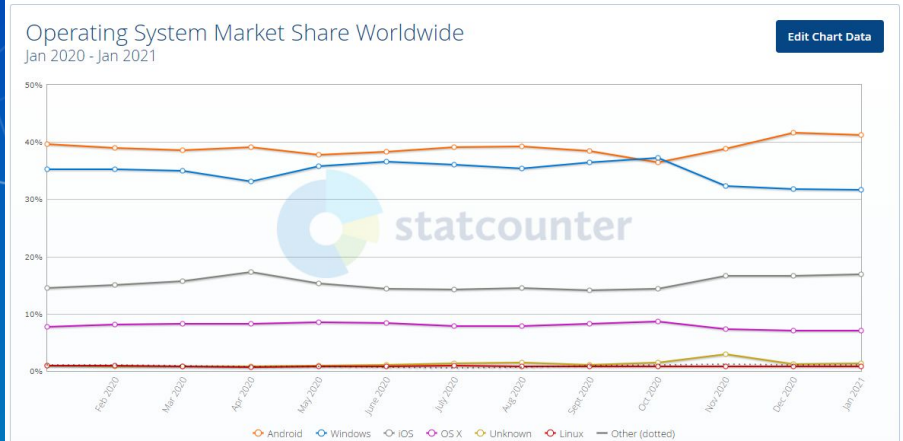
1. Windows Systems Information
2. Install Server Experience
3. Services
   a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. HW

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

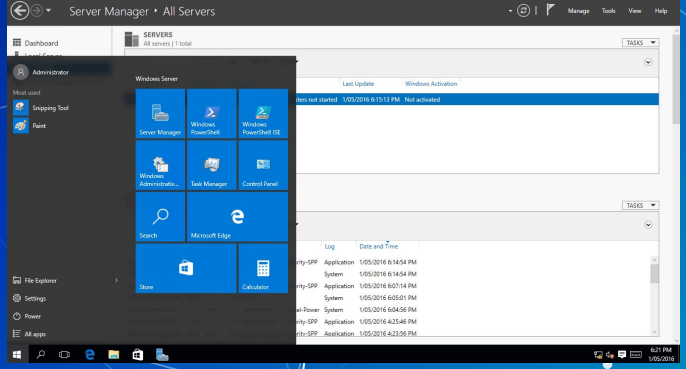
Android	Windows	iOS	OS X	Unknown	Linux
41.28%	31.6%	16.89%	7.01%	1.31%	0.8%

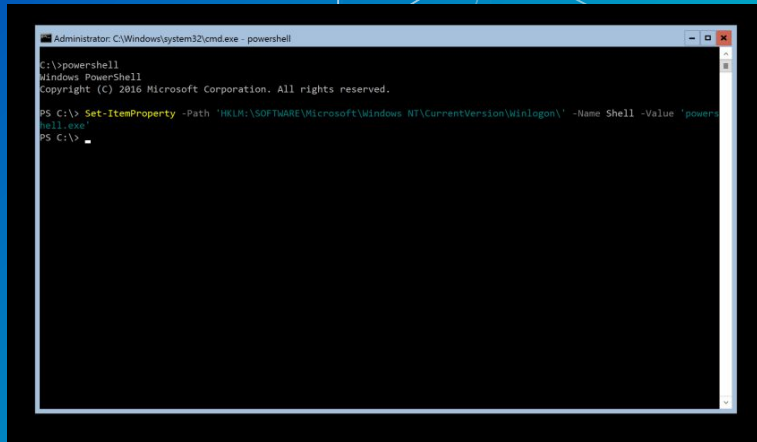
Operating System Market Share Worldwide - January 2021



Windows Server(s)

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





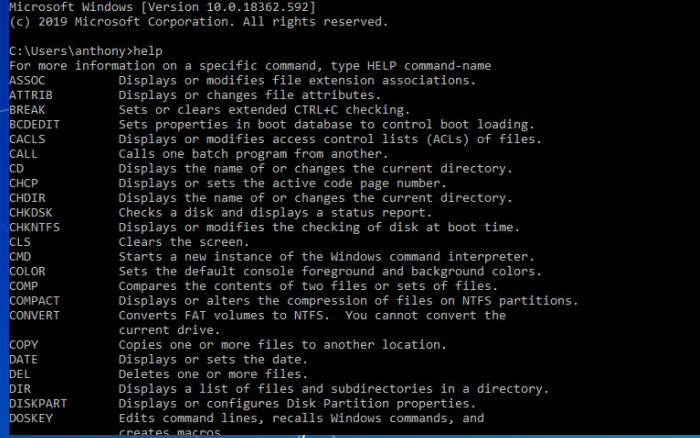
Windows Kernel

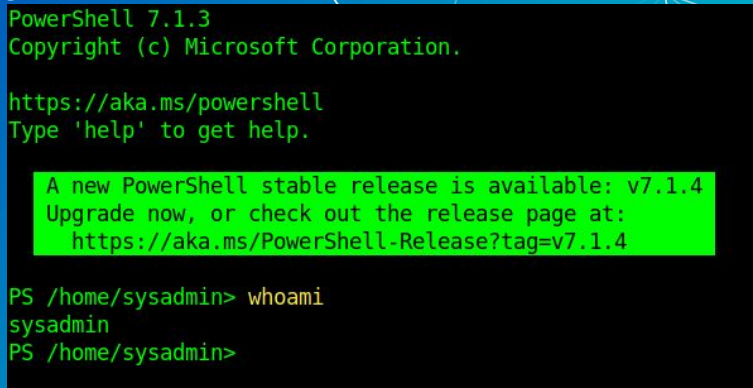
- The kernel is the part of the OS that talks to the hardware
- Has the highest privileges on the system
  - User < Administrator < System/Kernel
- Runs from a pre-existing account

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

Command Lines

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





Agenda

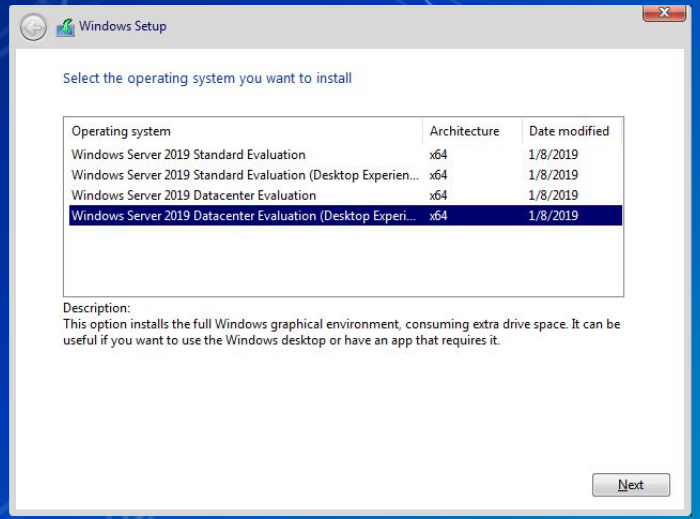
1. Windows Systems Information
2. Install Server Desktop Experience
3. Services
    a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. HW

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 cont.
7. Group Policy
8. HW

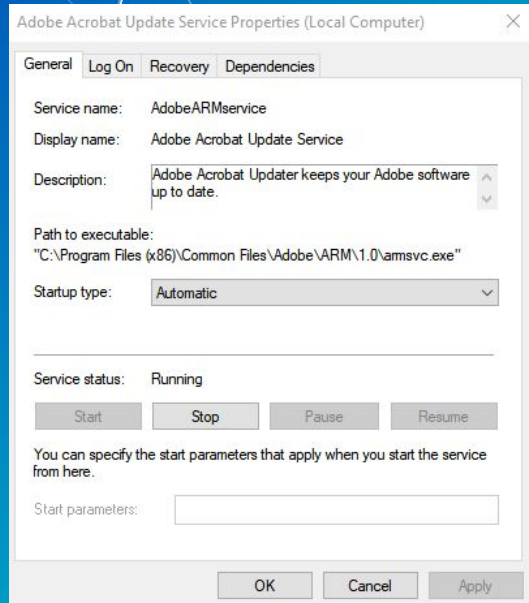
Services

- Services are processes that run in the background
- Typically manage things that make the system work
  - Networking, Update manager
- 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)".
```

```
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
```



Windows Server Services

- Windows Server provides a lot of services
  - File Transfer Protocol (FTP)
  - Web Server
    - Internet Information Service (IIS)
  - Server Message Block (SMB)
    - Network file share / Shared drive
  - Domain Name System (DNS)
  - Dynamic Host Configuration Protocol (DHCP)
  - 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. 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

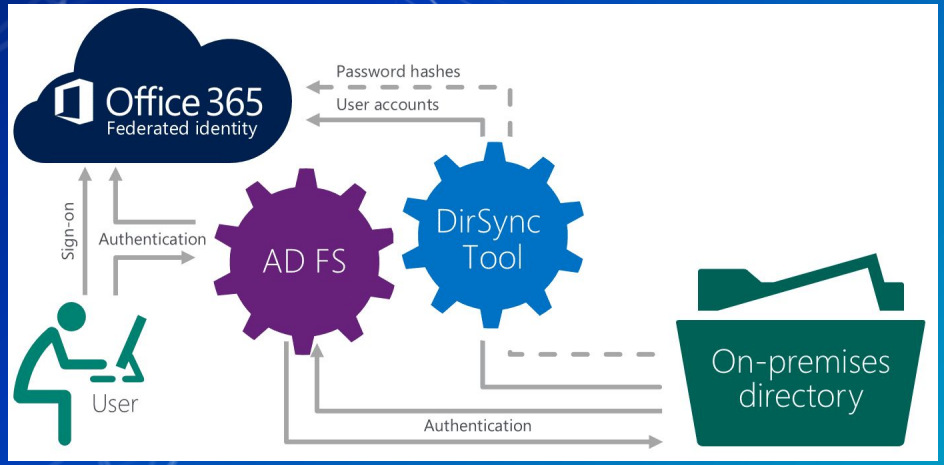
- Part of the Zero Trust Security Philosophy
  - Never trust that a user is who they say they are
  - Always verify the user's identity and level of access
- Multi-Factor Authentication (MFA) components:
  - Something the user knows
  - Something the user has
  - Something the user is
- Case in point: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

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

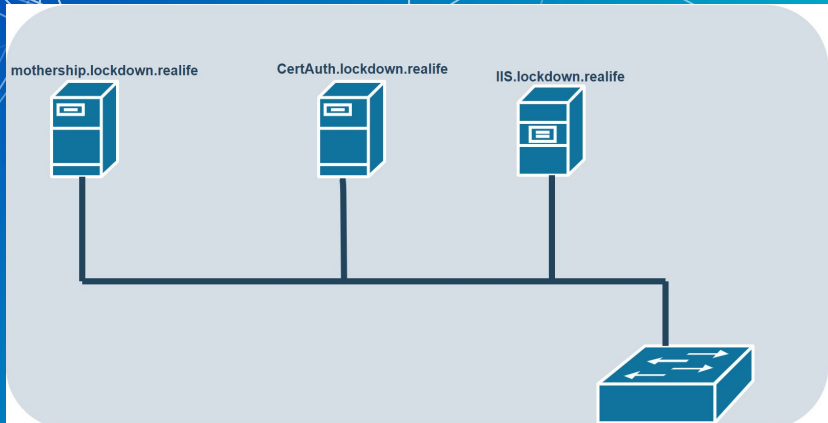
How does this work with AD?

- 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



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



QUESTIONS?

IAM can be complicated, but powerful.

Agenda

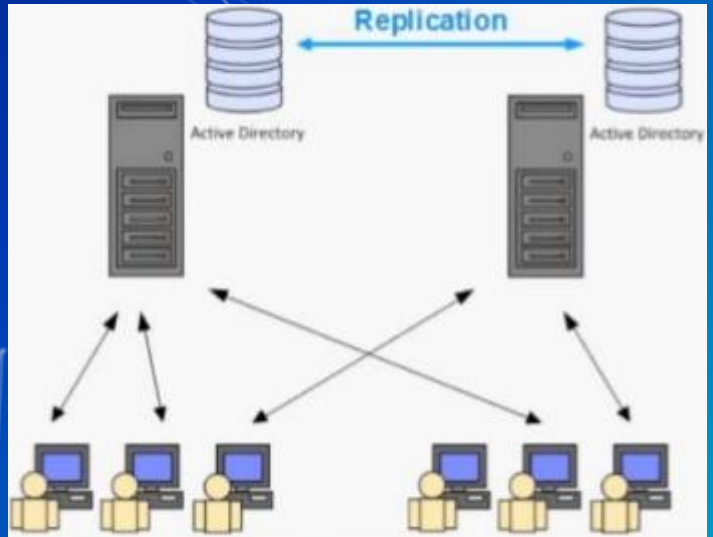
1. Windows Systems Information
2. Install Server Experience
3. Services
    a. IAM
4. The Domain Controller
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. HW

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



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. HW

Hands On

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

Break

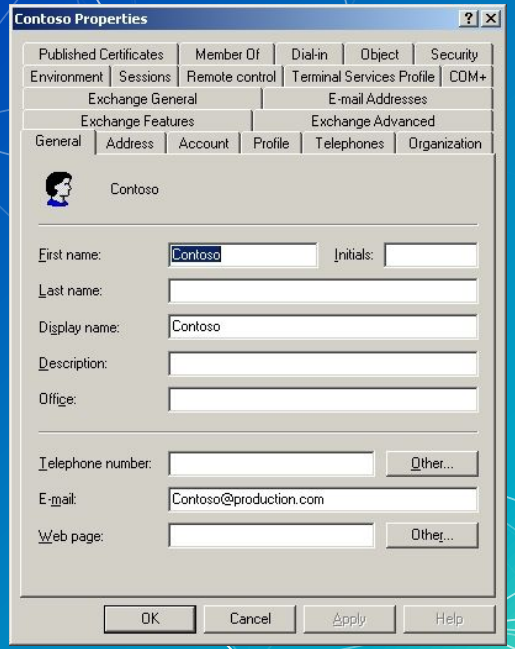
Please return in 10 mins

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. HW

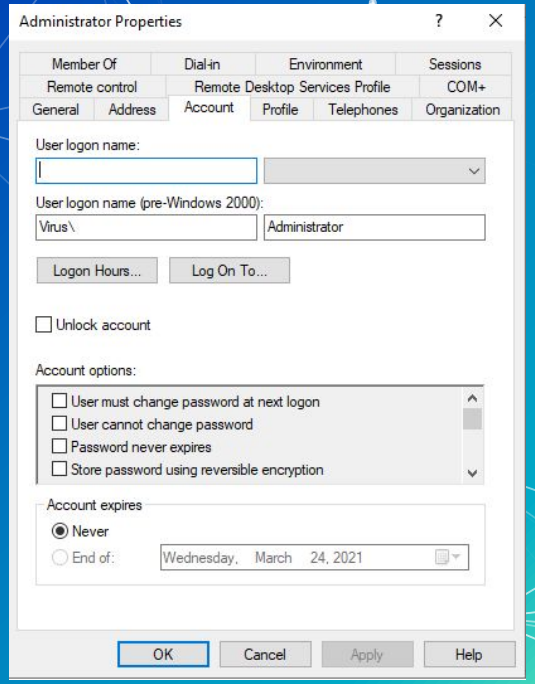
Active Directory - User Objects

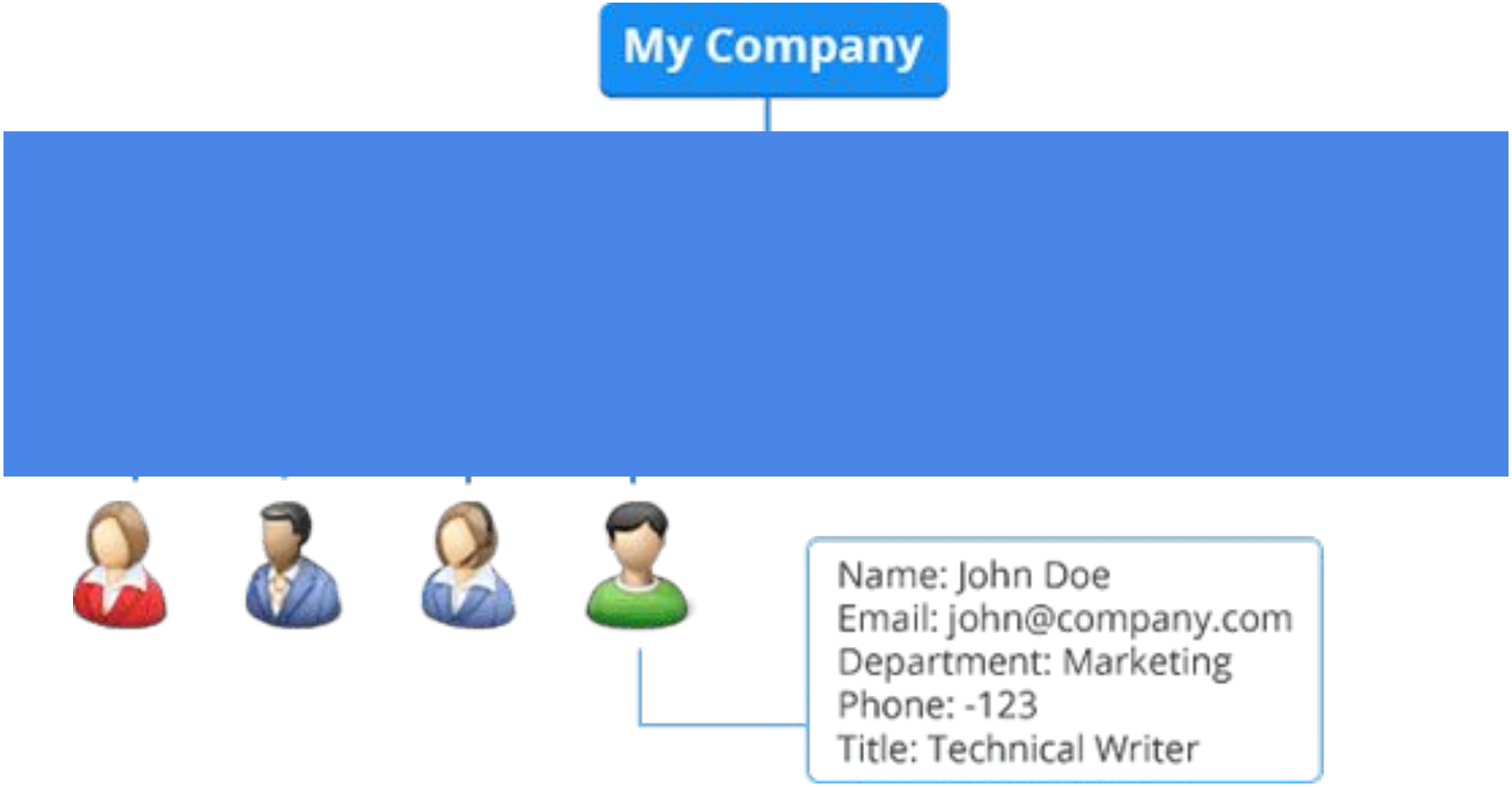
- What people authenticate against when they sign on
- Stores information on user
  - **Username***
  - Display name
  - Email
  - Phone number
  - Address
  - Location in organization
  - **Password (hashed)**



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




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

Active Directory - Security Groups

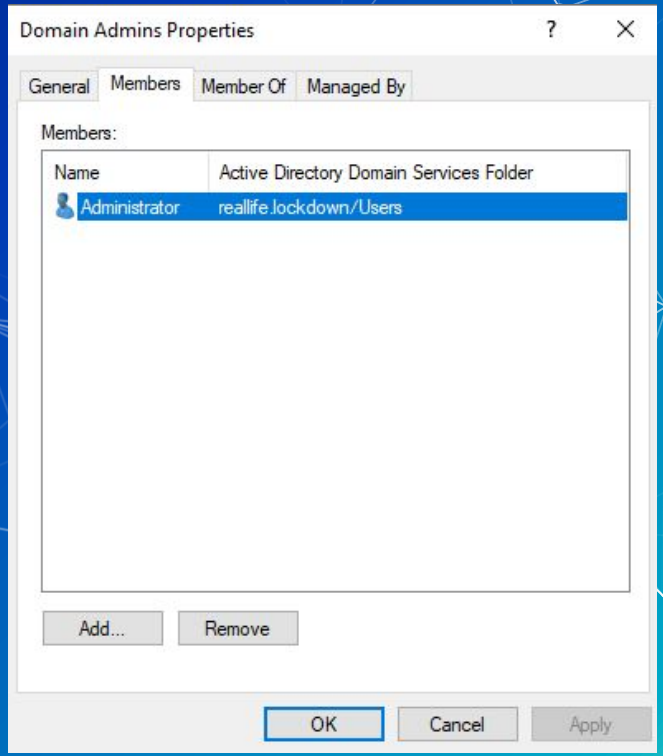
- We need a new object for each user. -> Too many to safely manage
  - UB has about 50,000 users on its main domain
- Security issues:
  - What happens when someone leaves?
  - What happens when we need to change permissions on every single student (~30K)
- Use Groups instead!

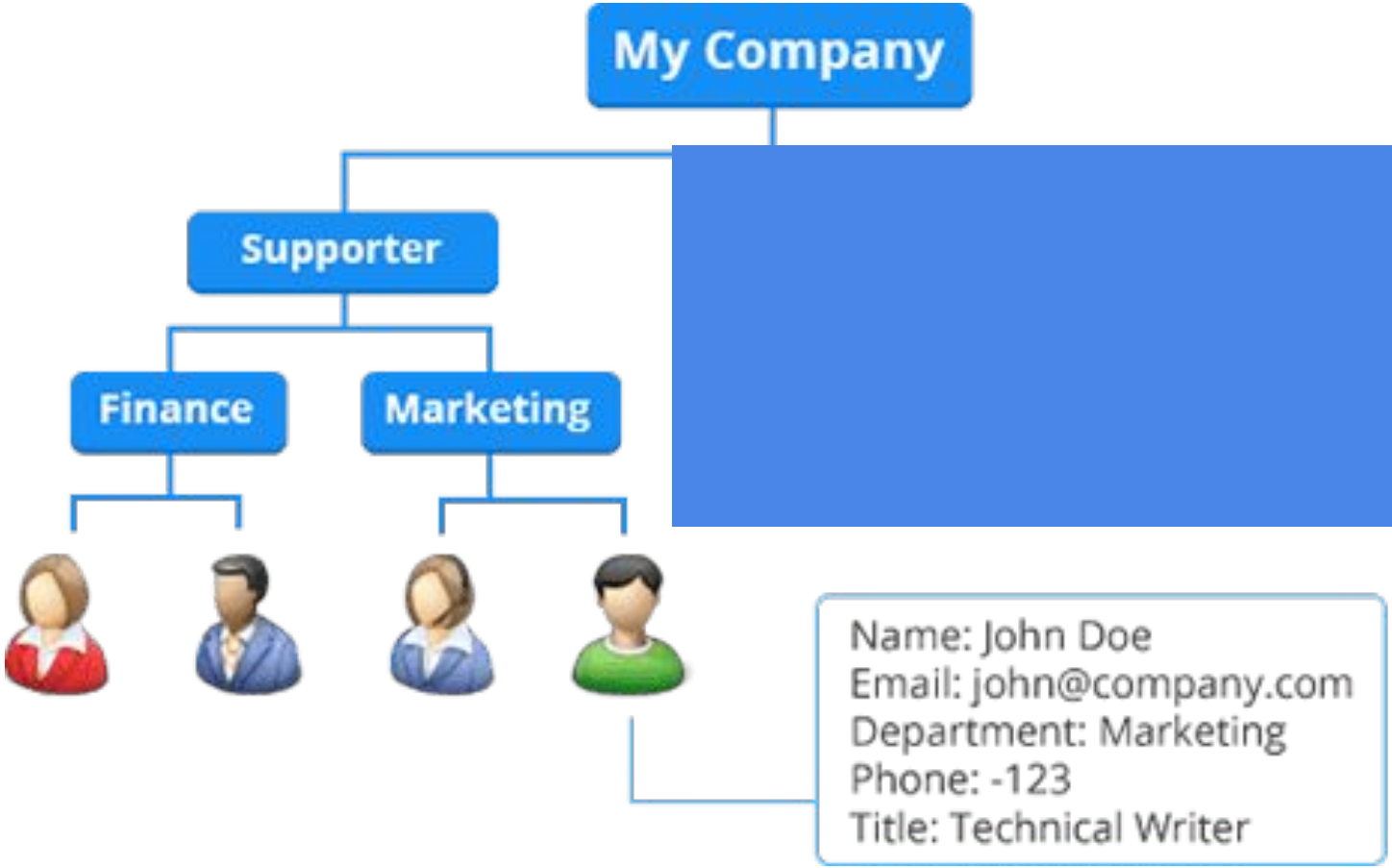
Active Directory - Security Groups

- 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
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

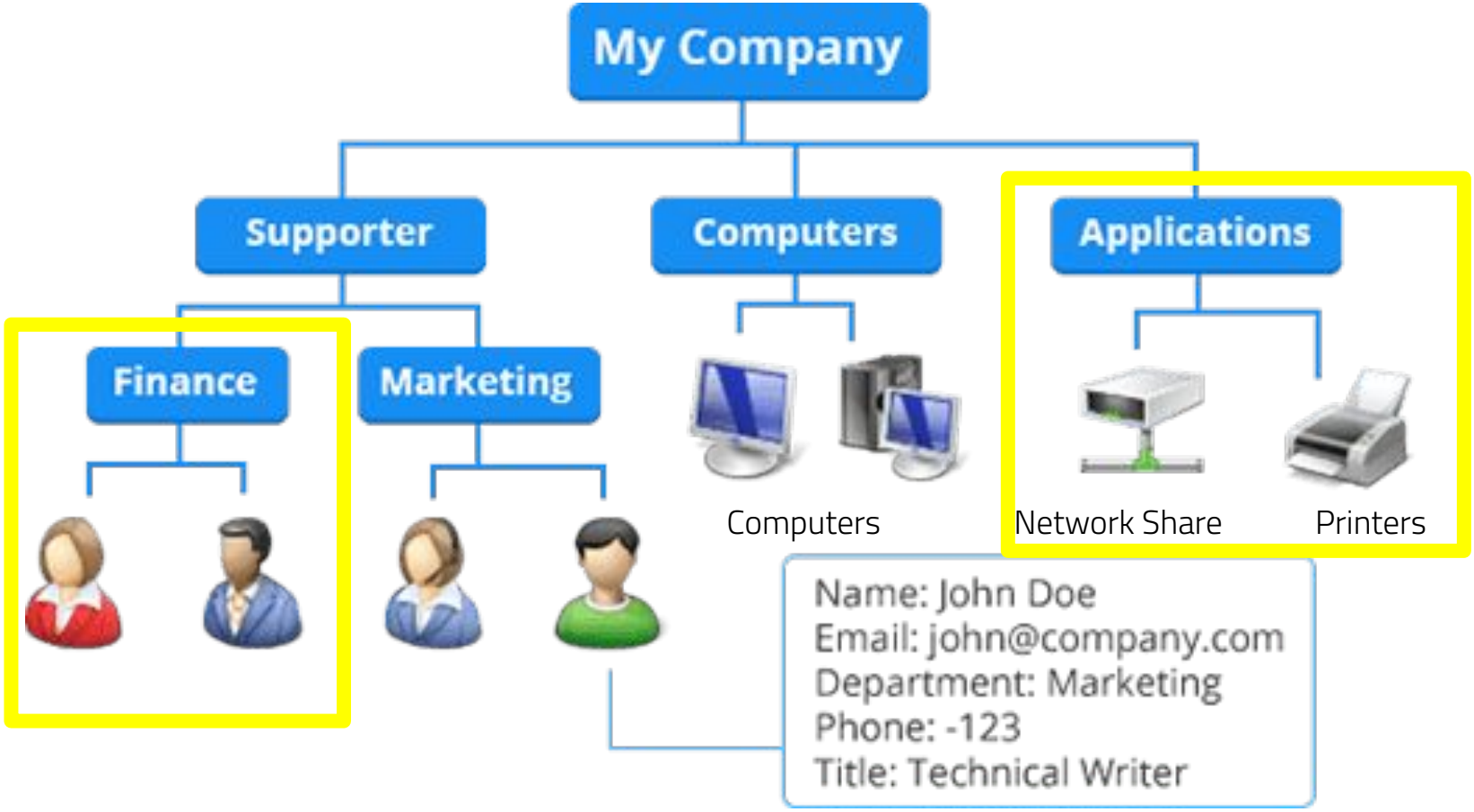
User Objects

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

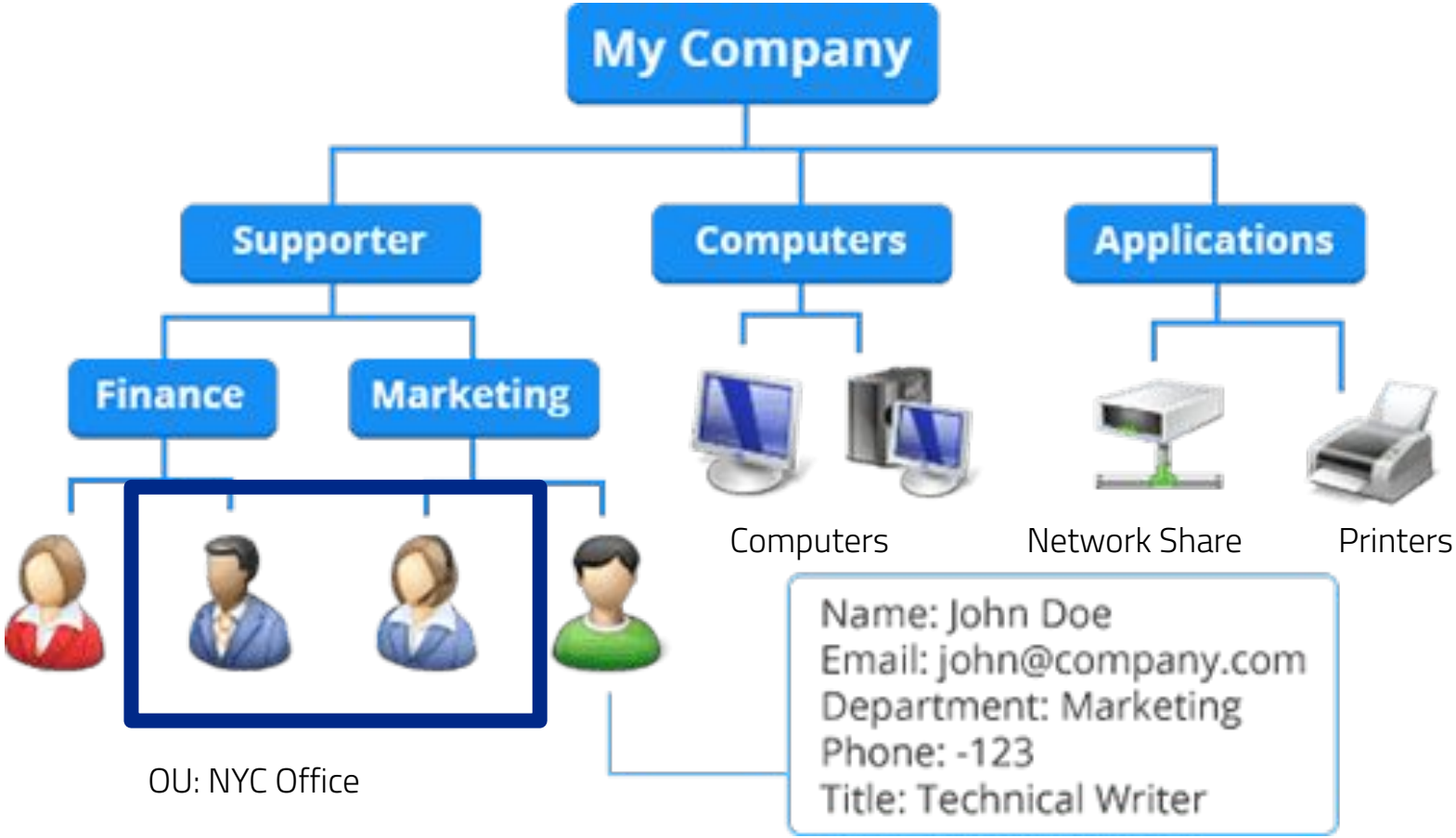

My Company
Supporter
Computers
Applications
Finance
Marketing
Computers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

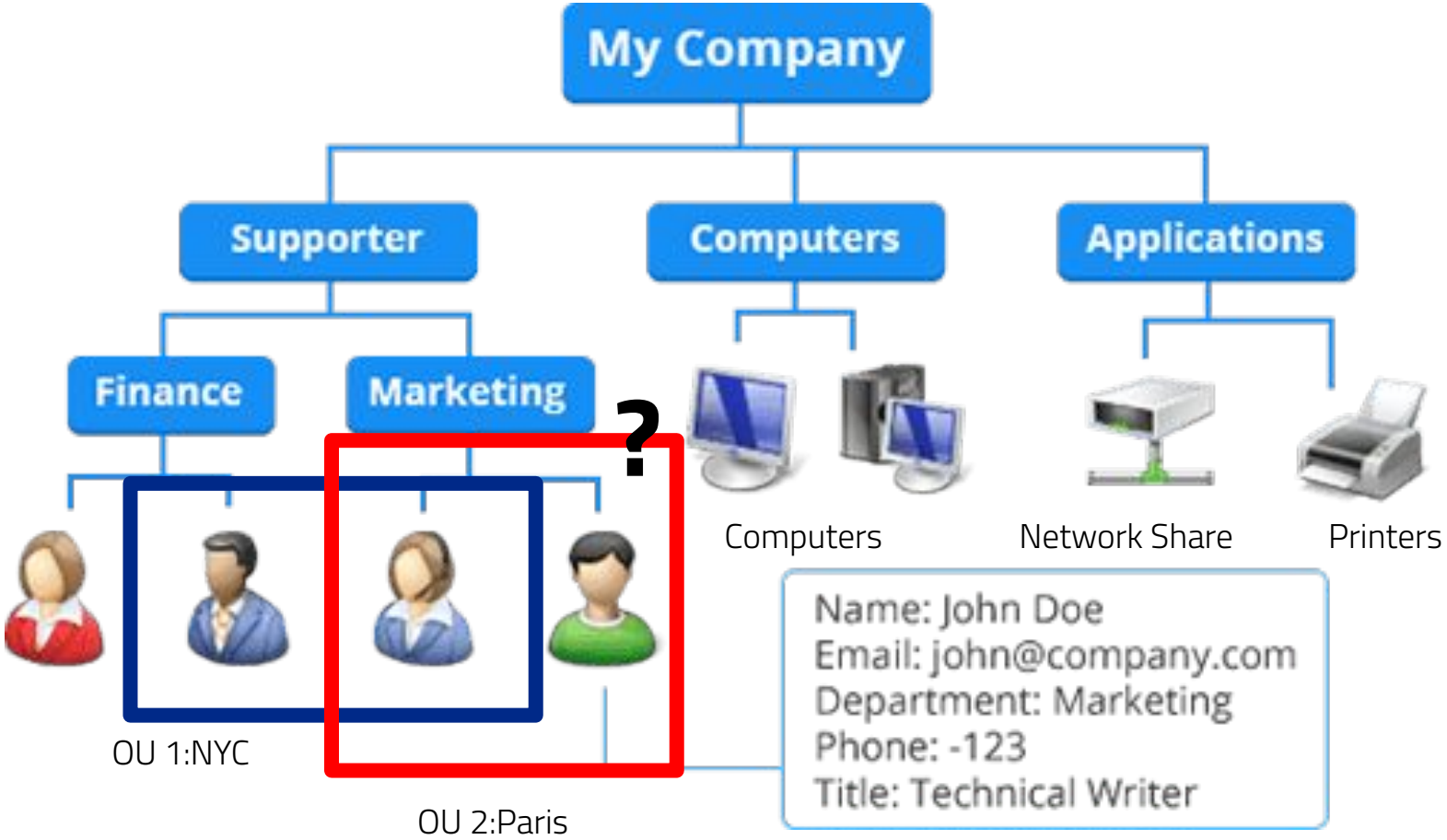
Active Directory - Introduction to OUs

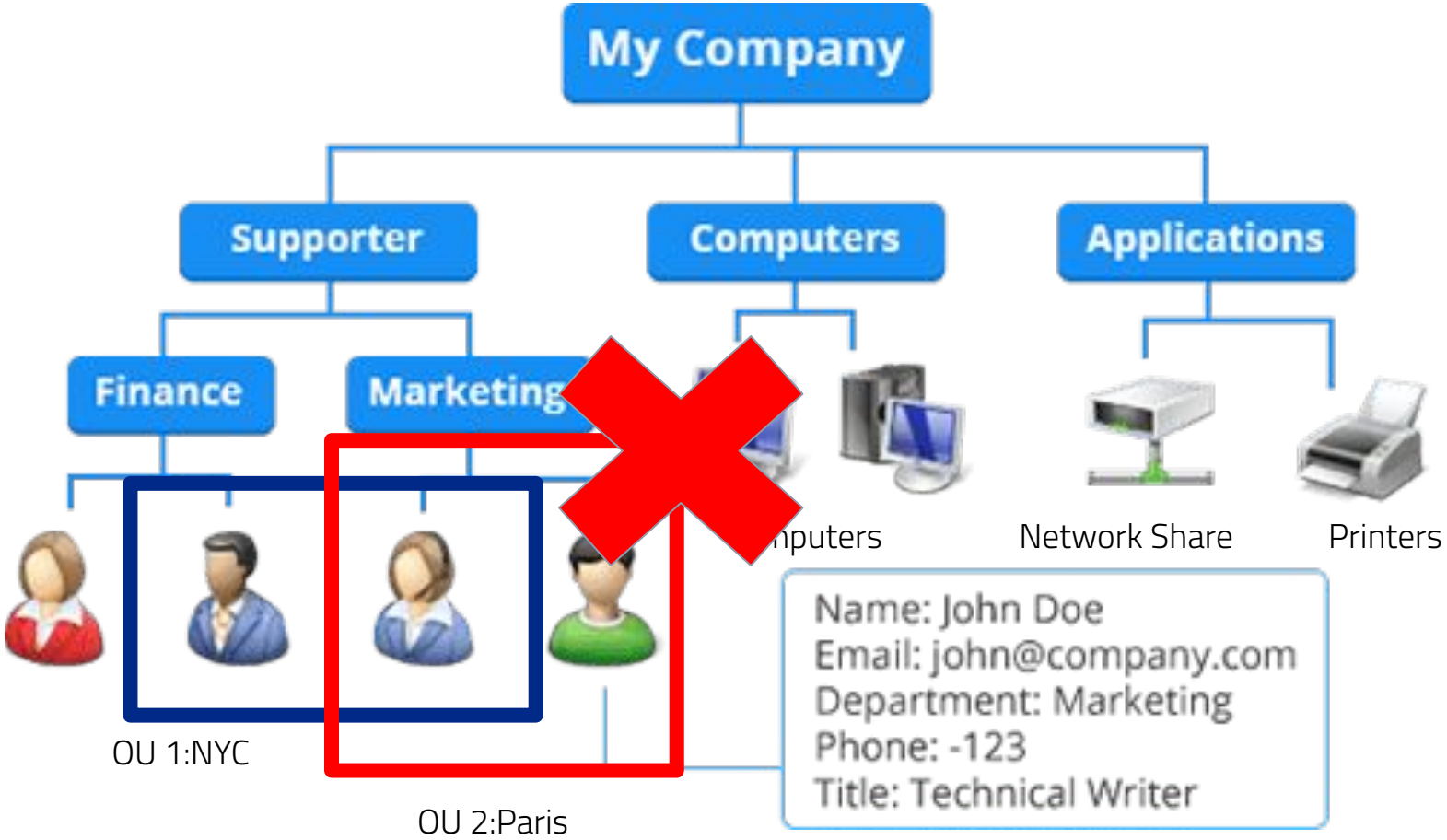
- Let's say we want to do something special for the UB Students, but don't want to mess with security permissions.
- All members of the student security group at UB can log into computers.
  - This is an IAM use case
- We want the SEAS Students get a picture of Davis as their background.
- The SOM Students 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.

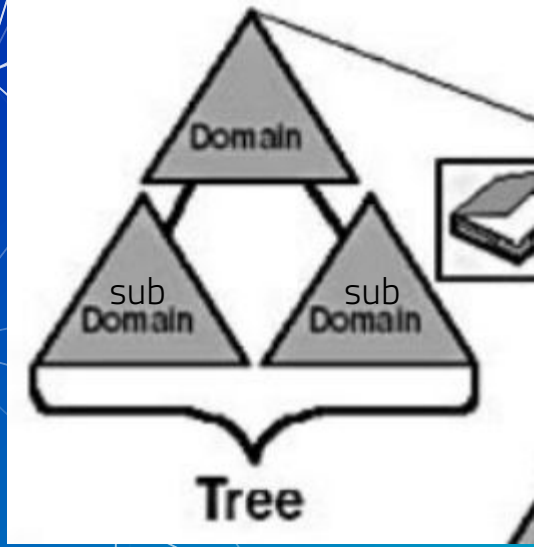

My Company
Supporter
Computers
Applications
Finance
Marketing
Computers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer
OU: NYC Office


My Company
Supporter
Computers
Applications
Finance
Marketing
?
Computers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer
OU 1:NYC
OU 2:Paris


My Company
Supporter
Computers
Applications
Finance
Marketing
nputers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer
OU 1:NYC
OU 2:Paris

Active Directory - Trees

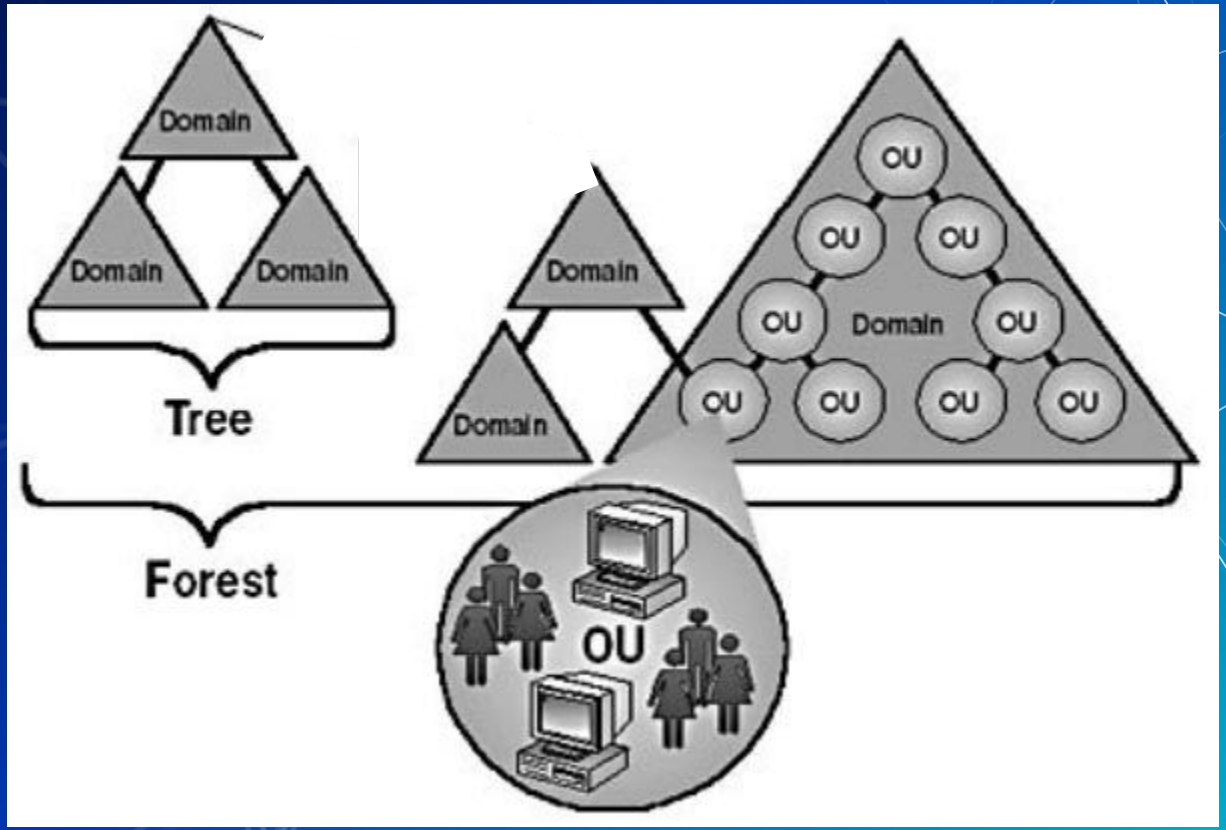
- Let's say we have a domain called company.xyz
  - company.xyz (domain) is composed of multiple objects
- company.xyz has 2 subdomains associated with it.
  - finance.company.xyz
  - marketing.company.xyz
- Each subdomain can be used to further **organize** the objects associated with company.xyz
-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

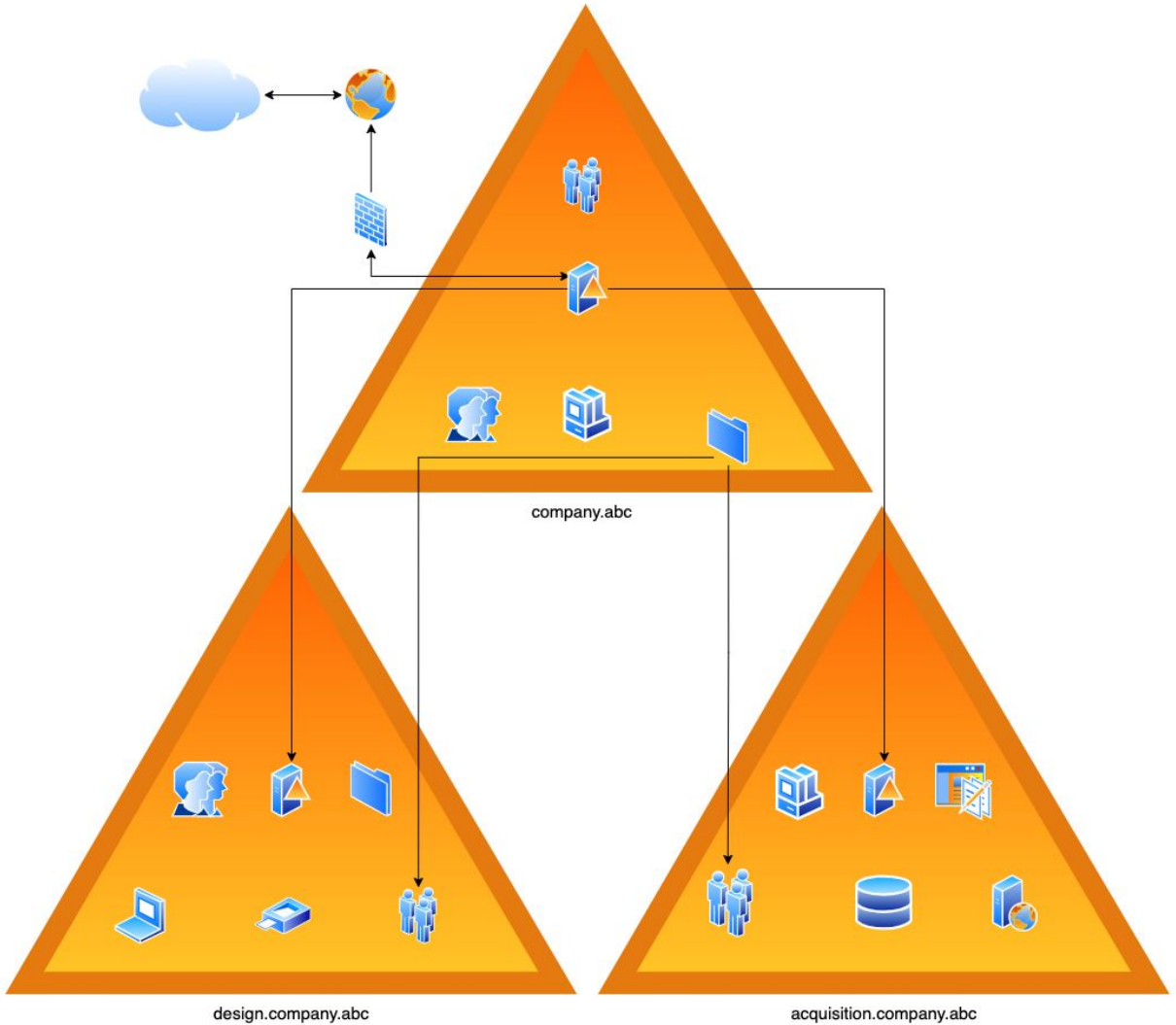


Active Directory - Forests

- 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


Domain
Domain
Domain
Tree
Domain
Domain
OU
OU
OU
OU
Domain
OU
OU
OU
OU
OU
Forest
OU


company.abc
design.company.abc
acquisition.company.abc

Confused? TL;DR

- 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?

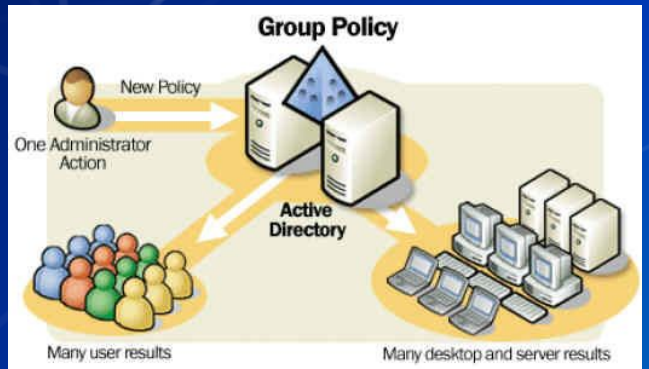
Too many acronyms.

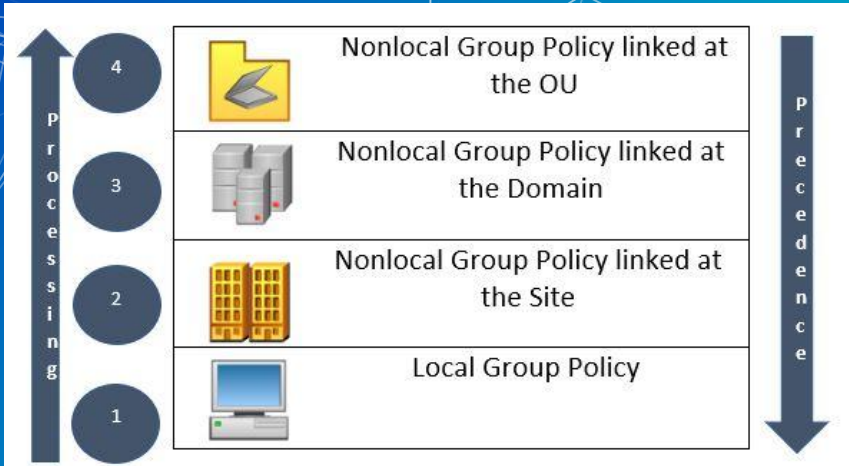
Agenda

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. 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
- Works via filtering
  - We want all X to follow this policy



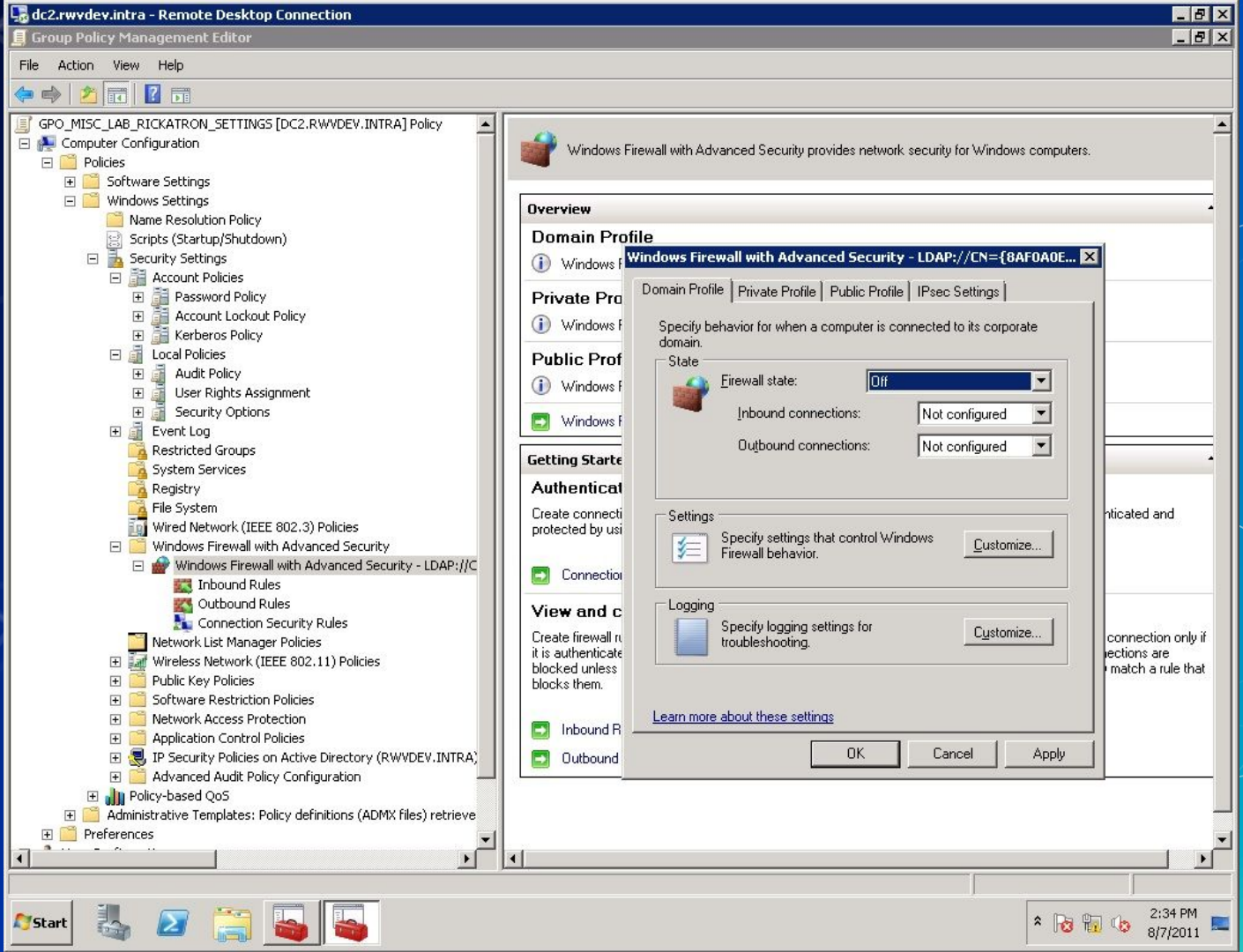


Group Policy Key Terms

- 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
    - < 4GB RAM
- Group Policy Object (GPO)
  - A set of rules that can be applied to any object

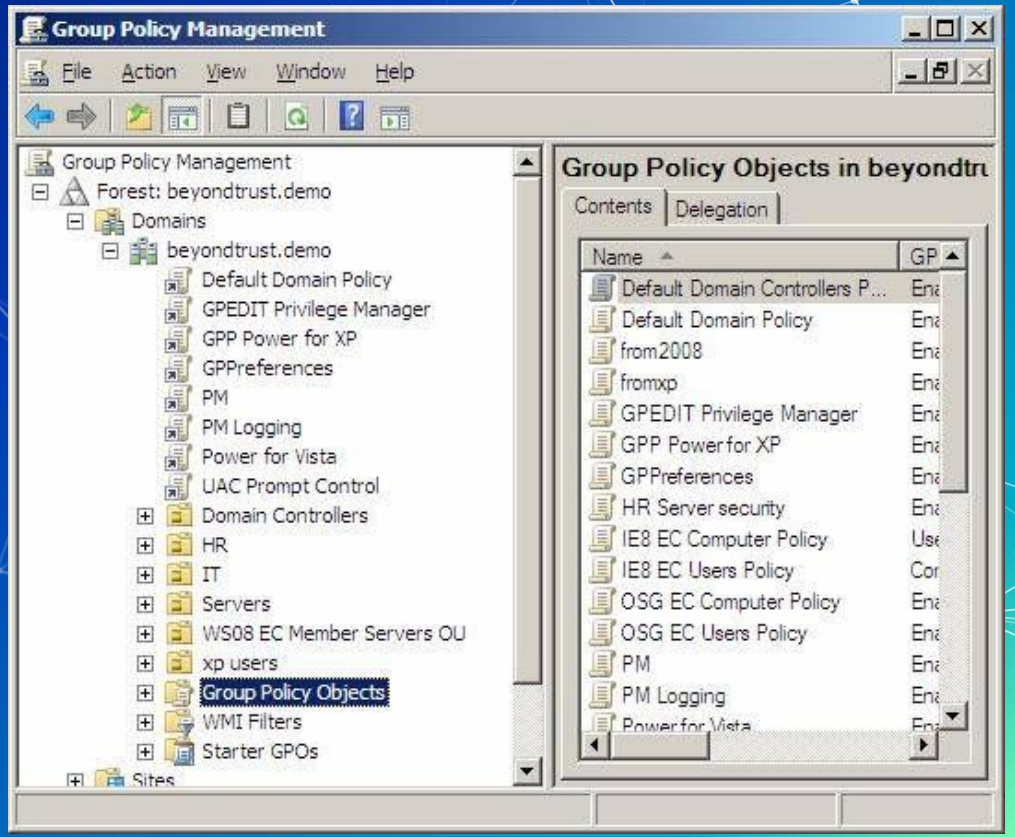
Group Policy Examples

- 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


dc2.rwvdev.intra - Remote Desktop Connection
Group Policy Management Editor
File Action View Help
GPO_MISC_LAB_RICKATRON_SETTINGS [DC2.RWVDEV.INTRA] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - LDAP://C
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (RWVDEV.INTRA)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieve
Preferences
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows F
Private Pro
Windows F
Public Prof
Windows F
Windows F
Getting Starte
Authenticat
Create connecti
protected by usi
Connectio
View and c
Create firewall r
it is authenticate
blocked unless
blocks them.
Inbound R
Outbound
nticated and
connection only if
ections are
match a rule that
Windows Firewall with Advanced Security - LDAP://CN={8AF0A0E...
Domain Profile
Private Profile
Public Profile
IPsec Settings
Specify behavior for when a computer is connected to its corporate domain.
State
Firewall state:
Off
Inbound connections:
Not configured
Outbound connections:
Not configured
Settings
Specify settings that control Windows Firewall behavior.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
Learn more about these settings
OK
Cancel
Apply
Start
2:34 PM
8/7/2011

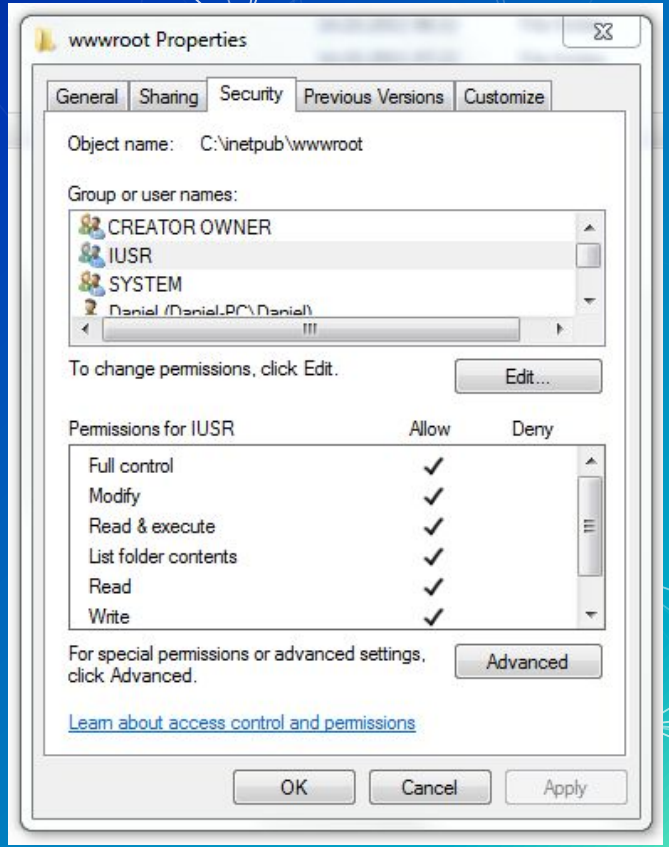
Multiple Group Policies

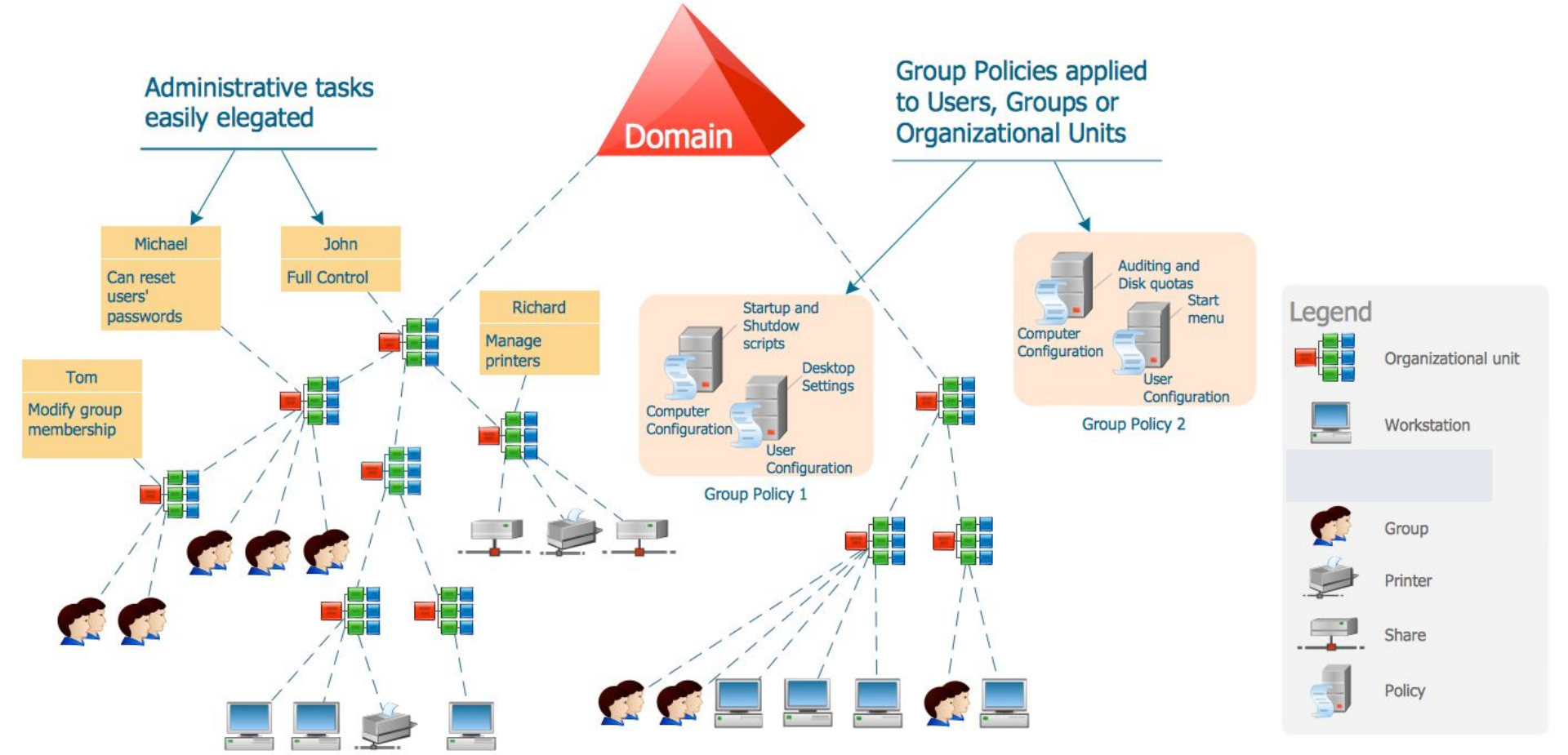
- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group



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




Administrative tasks easily elegated
Domain
Group Policies applied to Users, Groups or Organizational Units
Michael
Can reset users' passwords
John
Full Control
Richard
Manage printers
Tom
Modify group membership
Startup and Shutdow scripts
Desktop Settings
Computer Configuration
User Configuration
Group Policy 1
Auditing and Disk quotas
Start menu
Computer Configuration
User Configuration
Group Policy 2
Legend
Organizational unit
Workstation
Group
Printer
Share
Policy

Further Reading

What is IAM?

MS Docs: Understanding AD

MS Docs: Powershell Reference

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. HW

Homework