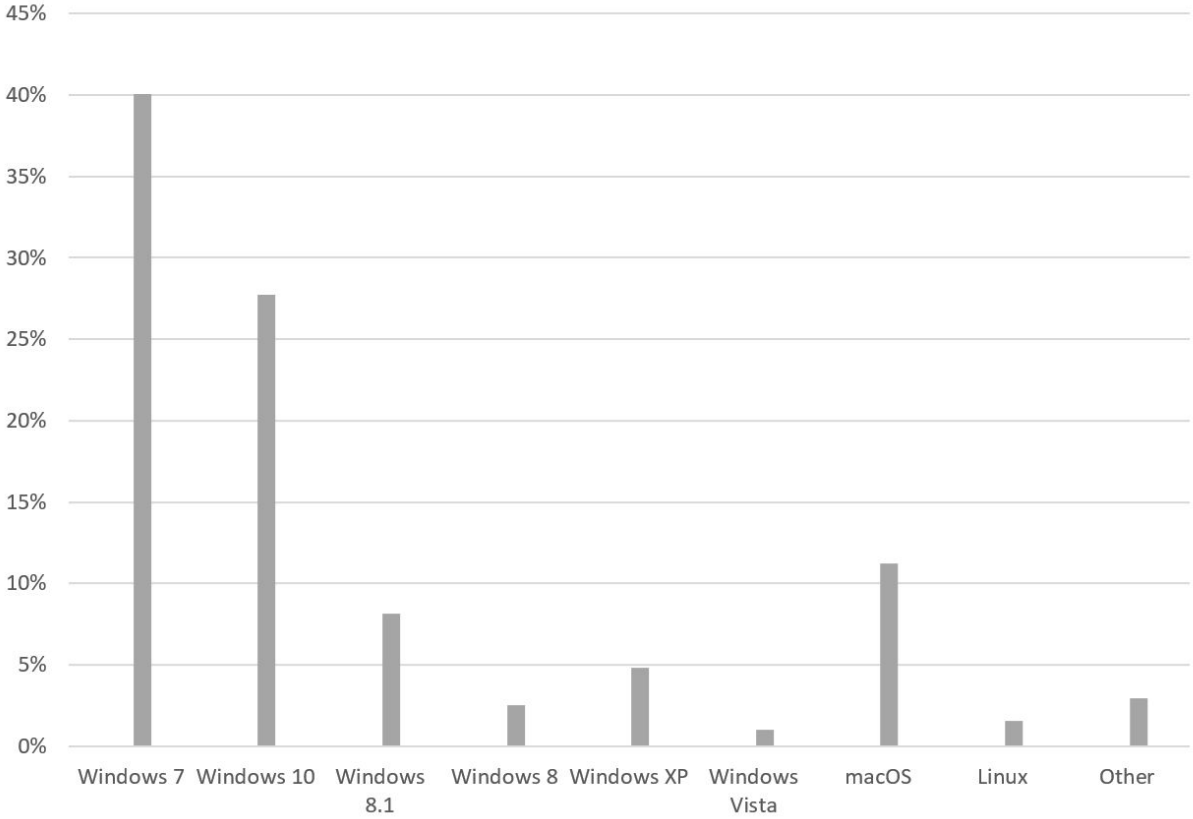
Windows

Not Just For Houses

Everyone Uses Windows!



Versions of Windows 10

- There are multiple different versions of Windows 10 that support different features
- The version of Windows that we will be using is Enterprise edition
- This supports features that are useful in controlling a Windows environment

Features	Home	Pro	Enterprise	Education
Device Encryption[6]	✓	✓	✓	✓
Domain Join		✓	✓	✓
Group Policy Management		✓	✓	✓
BitLocker[2]		✓	✓	✓
Enterprise Mode Internet Explorer (EMIE)		✓	✓	✓
Assigned Access 8.1		✓	✓	✓
Remote Desktop		✓	✓	✓
Direct Access			✓	✓
Windows To Go Creator			✓	✓
AppLocker			✓	✓
BranchCache			✓	✓

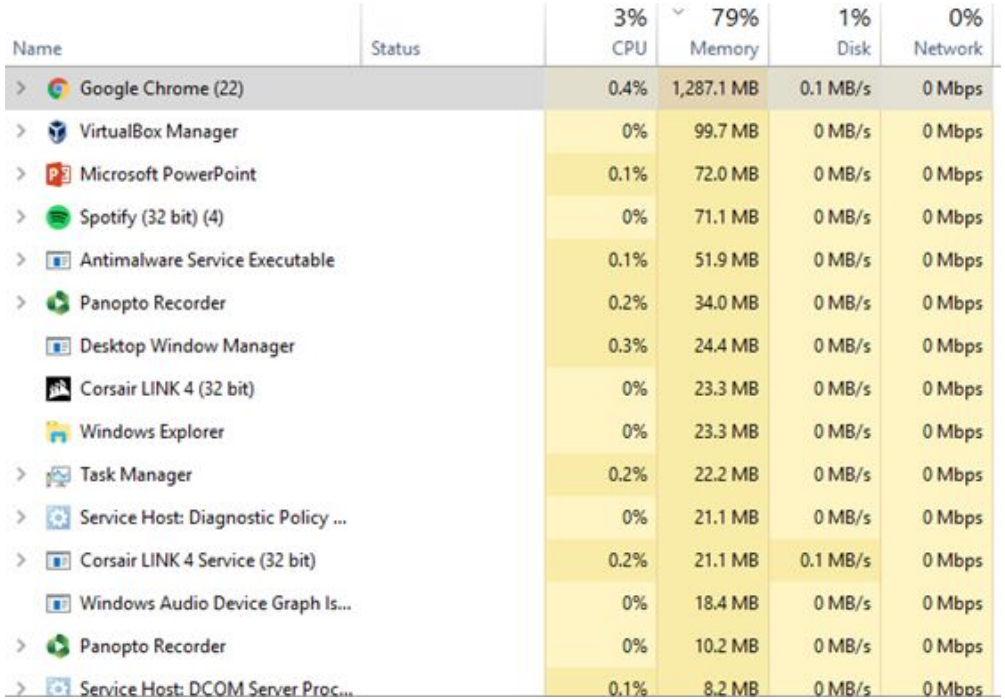
Users

- Accounts to separate people on a computer
- Multiple user accounts on a computer
  - Ex) shared family computer
- Access level can be set differently for each user
  - Ex) parent administrative account vs child standard account
  - Limit what can be done or installed

Command: Control userpasswords2

Processes in windows

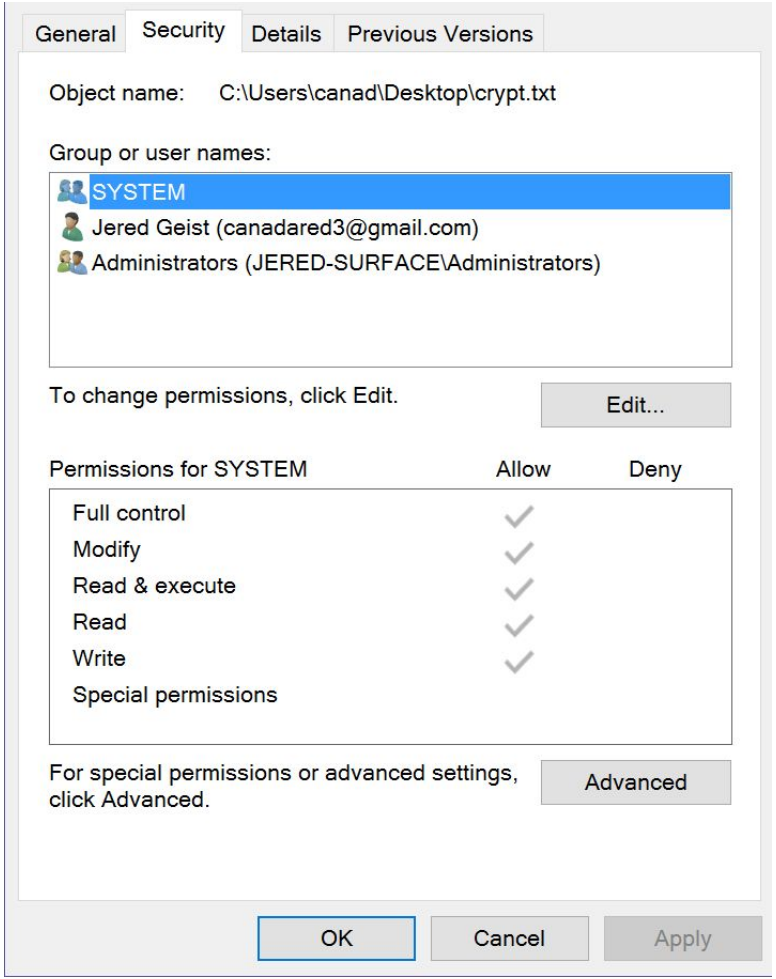
- A process in the simplest terms, is an executing program
- All programs on your computer including Windows programs is a process
- Programs in Windows are launched in the form of an executable which is located on disk



Name	Status	3% CPU	79% Memory	1% Disk	0% Network
Google Chrome (22)		0.4%	1,287.1 MB	0.1 MB/s	0 Mbps
VirtualBox Manager		0%	99.7 MB	0 MB/s	0 Mbps
Microsoft PowerPoint		0.1%	72.0 MB	0 MB/s	0 Mbps
Spotify (32 bit) (4)		0%	71.1 MB	0 MB/s	0 Mbps
Antimalware Service Executable		0.1%	51.9 MB	0 MB/s	0 Mbps
Panopto Recorder		0.2%	34.0 MB	0 MB/s	0 Mbps
Desktop Window Manager		0.3%	24.4 MB	0 MB/s	0 Mbps
Corsair LINK 4 (32 bit)		0%	23.3 MB	0 MB/s	0 Mbps
Windows Explorer		0%	23.3 MB	0 MB/s	0 Mbps
Task Manager		0.2%	22.2 MB	0 MB/s	0 Mbps
Service Host: Diagnostic Policy ...		0%	21.1 MB	0 MB/s	0 Mbps
Corsair LINK 4 Service (32 bit)		0.2%	21.1 MB	0.1 MB/s	0 Mbps
Windows Audio Device Graph Is...		0%	18.4 MB	0 MB/s	0 Mbps
Panopto Recorder		0%	10.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Proc...		0.1%	8.2 MB	0 MB/s	0 Mbps

Files

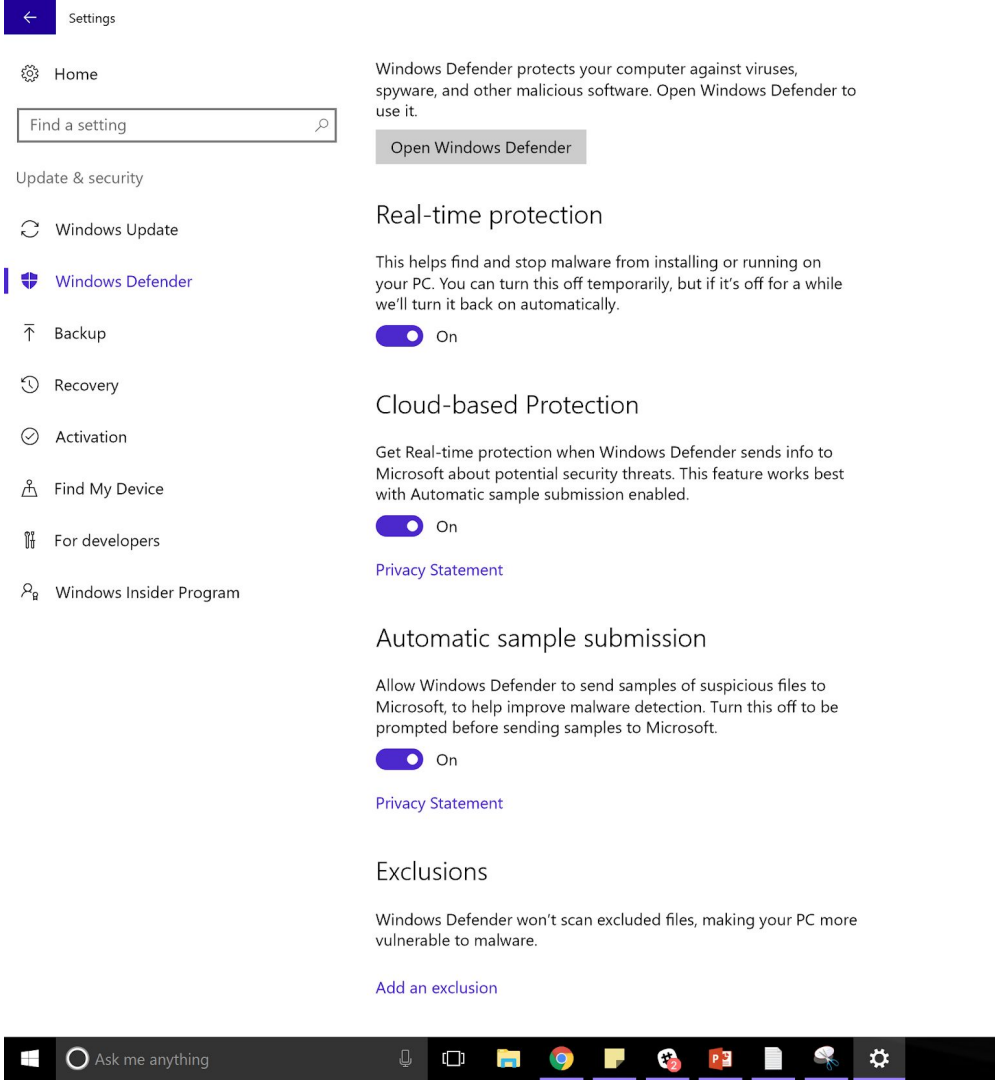
- Store digital data
- Security settings can be changed on files based on user accounts
- Can limit read, write, modify permissions
- Only allow certain people to view sensitive files
    - ex) tax information stored on family computer

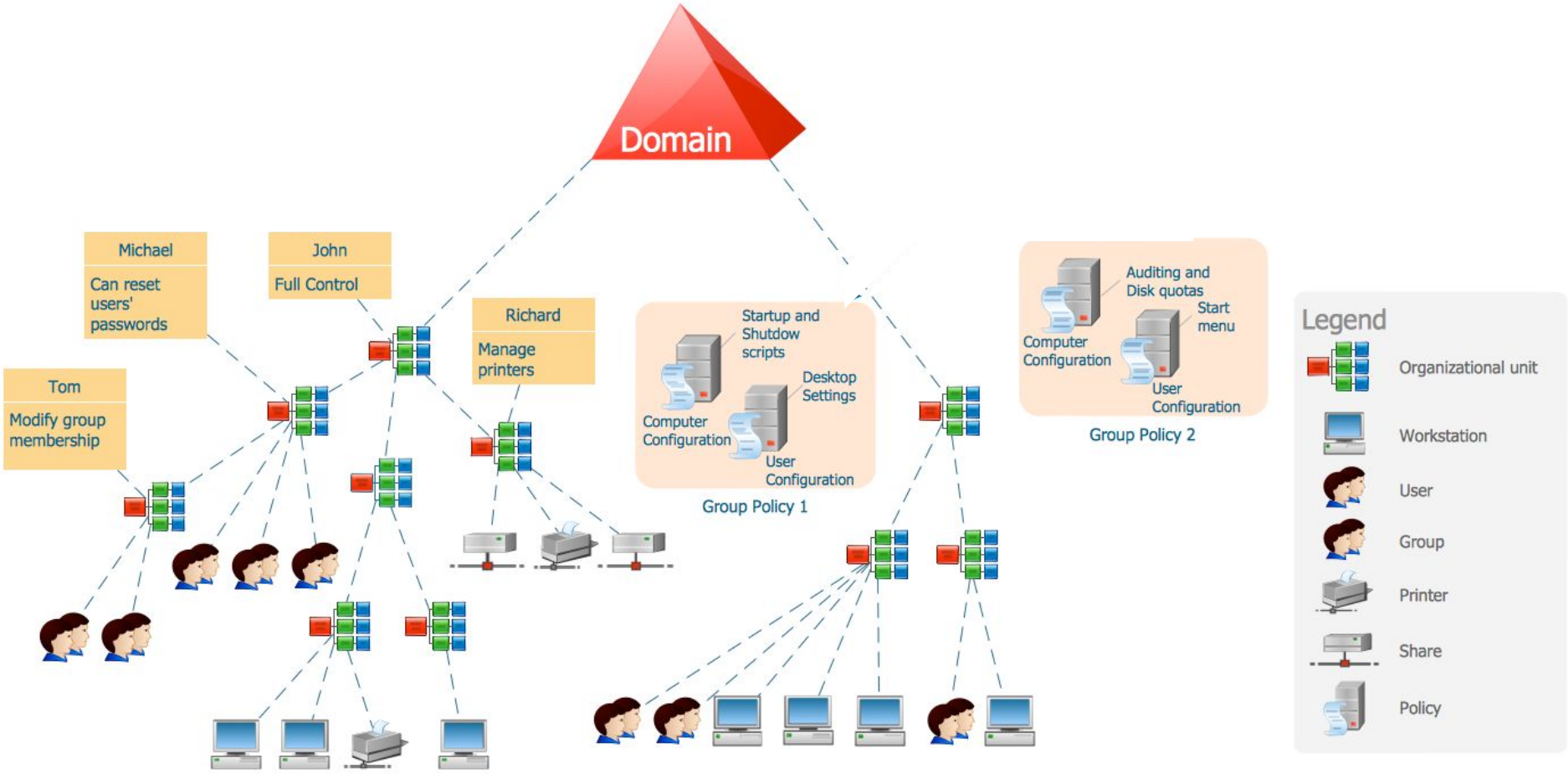


Right click on a file and go to properties

Settings

- Can change how your computer works
- Settings for everything!
  - Updates
  - anti -virus
  - Time zone
  - Brightness
  - etc.




Domain
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
User
Group
Printer
Share
Policy

Networks are complex

- Need easy way to manage everything
  - Centralized login authentication
  - File sharing
  - Printer sharing
  - File security

- Specialized tools for easier management
  - Active Directory
  - Open LDAP
  - Free IPA

Windows Server

What can it do?

Can take on many roles, just like linux

- Email
- File storage
- User privileges
- Authentication
- Website
- DNS
- Many more

Active Directory and Group Policy

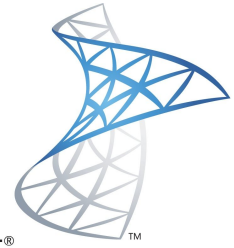
- Tools used for majority of windows based network management
- Interact and control many objects at once
  - Users
  - Computers
  - Files

Other Common Roles and Features

- SMB Server
- FTP Server
- Exchange Server
- Firewall
- Application deployment
- Centralized monitoring
- VPN
- DNS
- IIS (web server)

Microsoft

IIS



Microsoft®
System Center

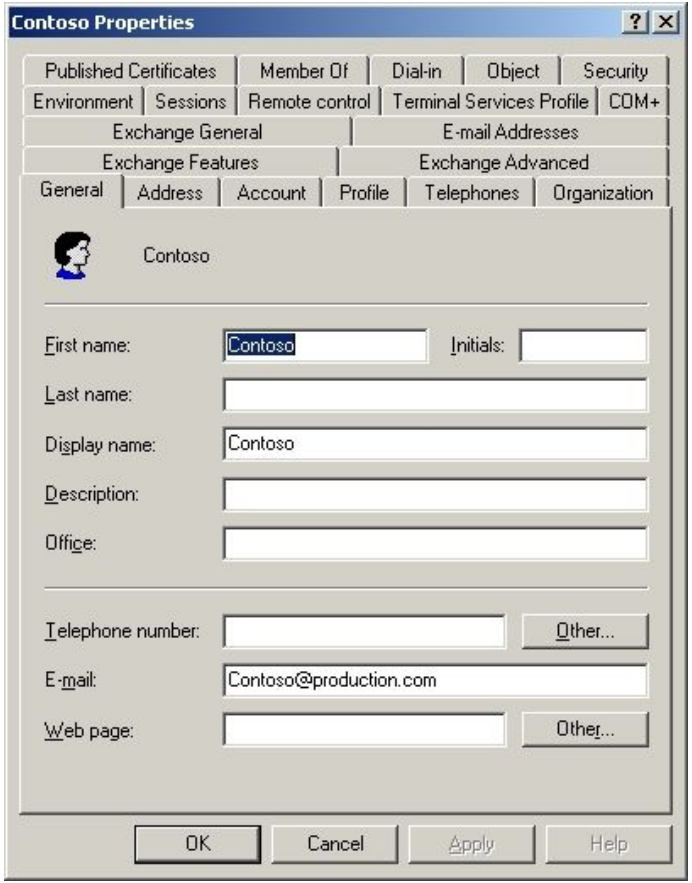
Microsoft®
Exchange

Active Directory

- Database of objects in a network (Domain)
  - Users
  - Computers
  - Printers
  - Security Groups
  - More
- Hosted on a Windows Server (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

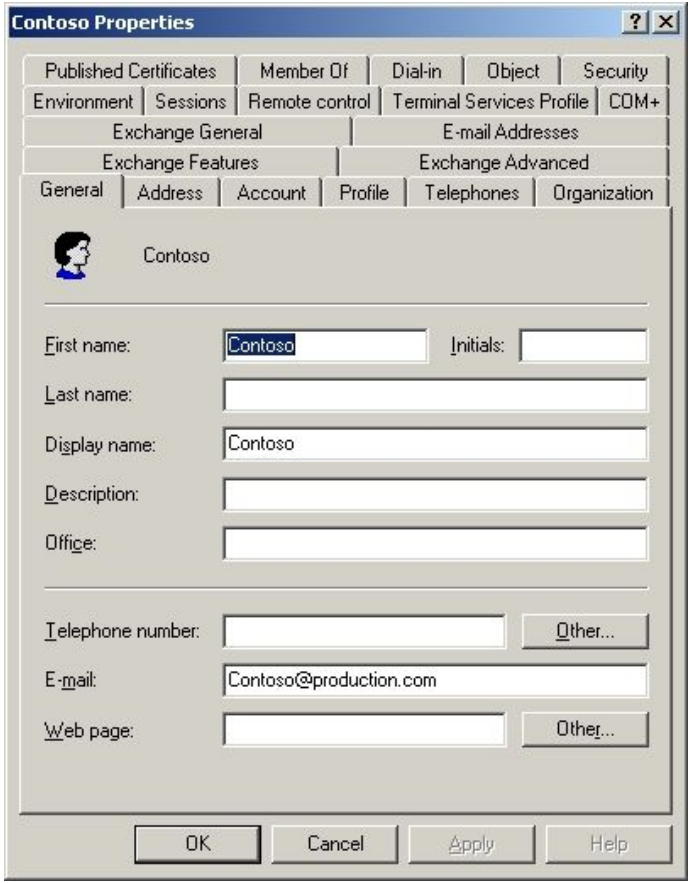
Users

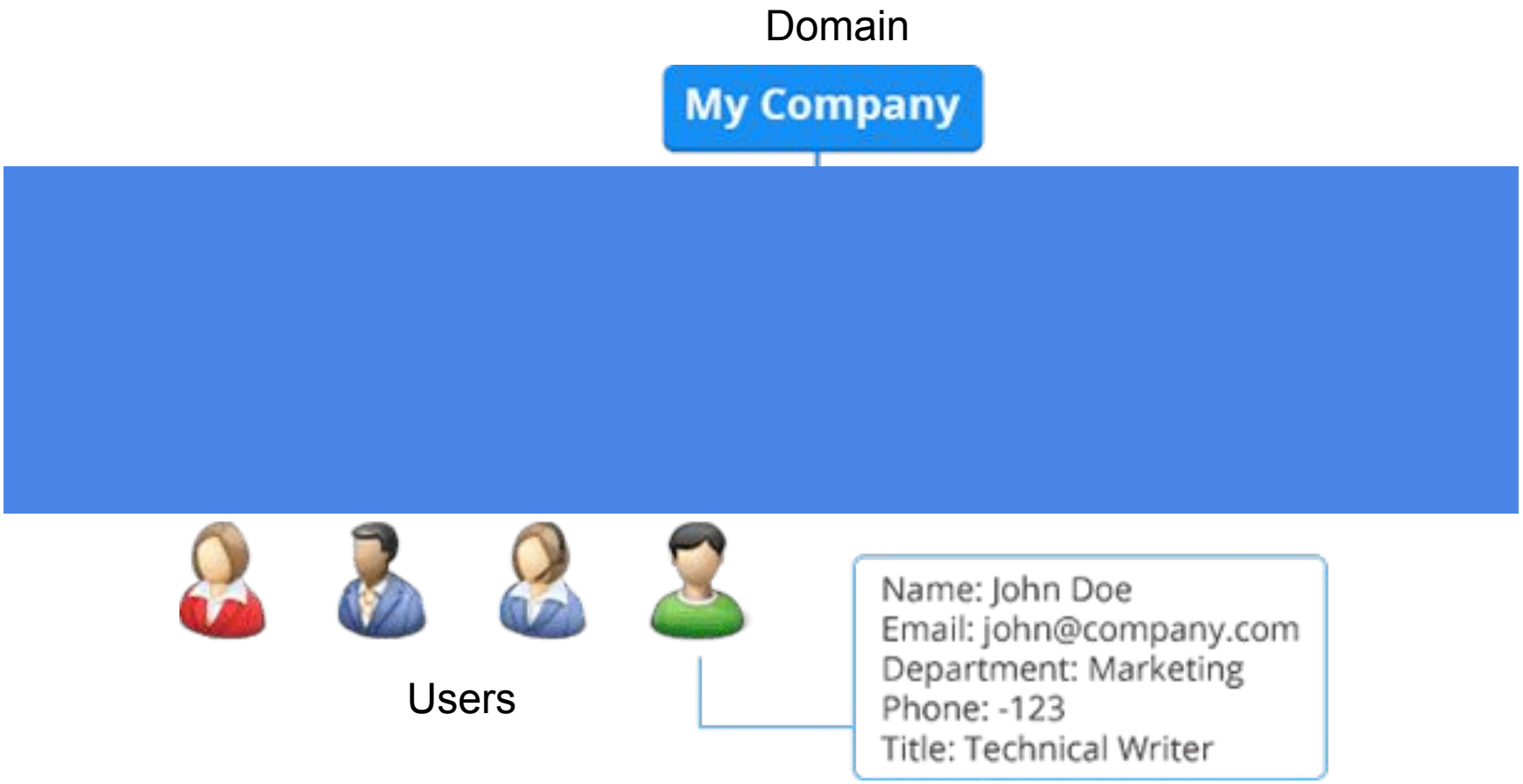
- Stores information on user
  - Name
  - Email
  - Phone number
  - Address
  - Location in organization
  - Password (hashed)

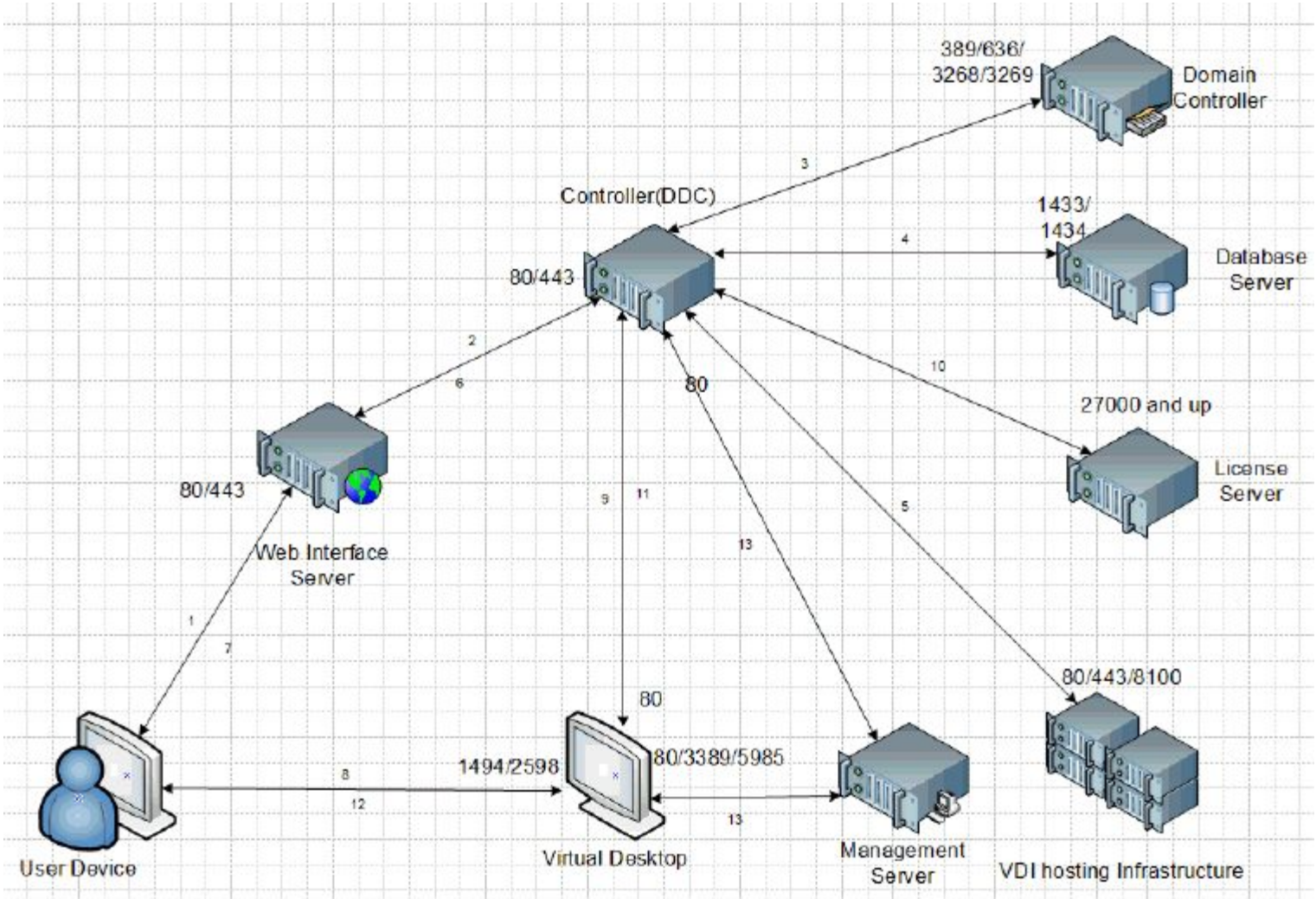


Users

- Controls permissions
  - File and folder access
  - VPN access
  - Password management
  - Active account
  - Access control
- Ability to control total network access
- Map drives to computer
- Folder redirection

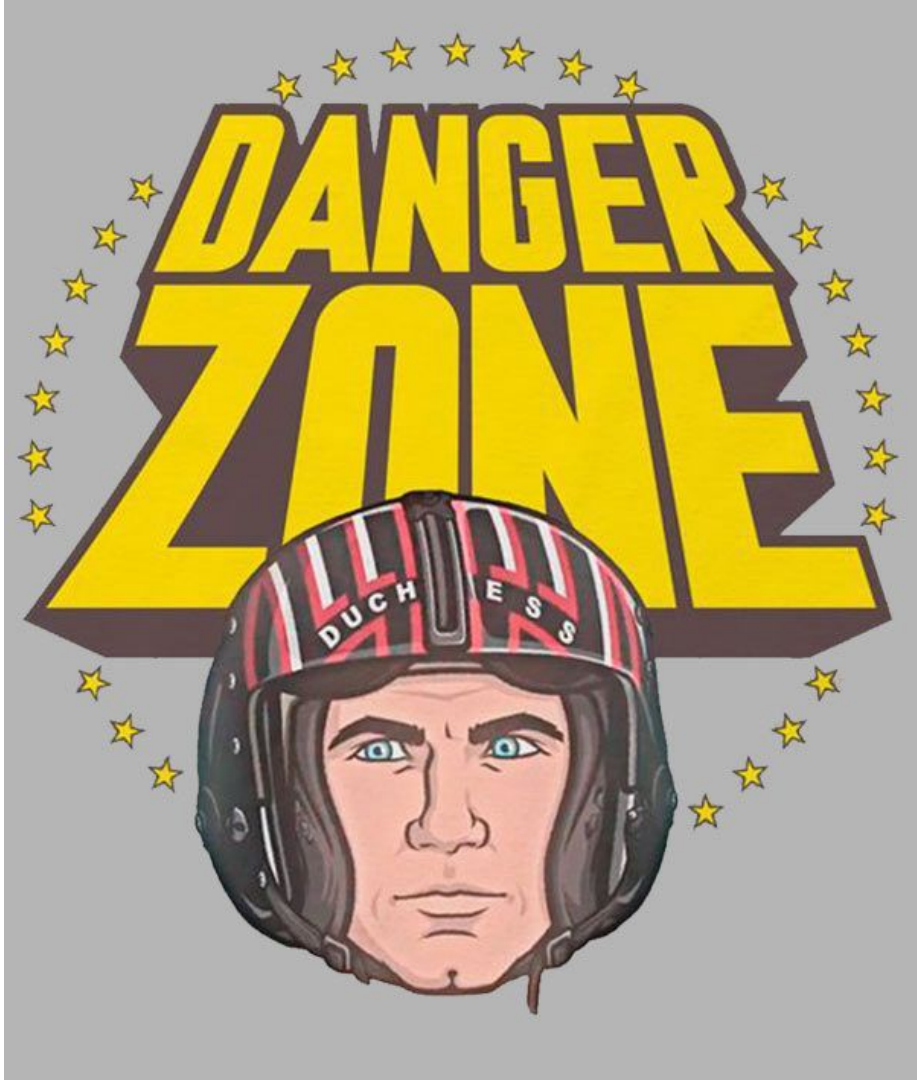



Domain
My Company
Users
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer


389/636/
3268/3269
Domain
Controller
3
Controller(DDC)
1433/
1434
4
80/443
Database
Server
2
6
10
80
27000 and up
License
Server
80/443
9
11
5
13
Web Interface
Server
1
7
80
80/443/8100
1494/2598
80/3389/5985
8
12
13
User Device
Virtual Desktop
Management
Server
VDI hosting Infrastructure

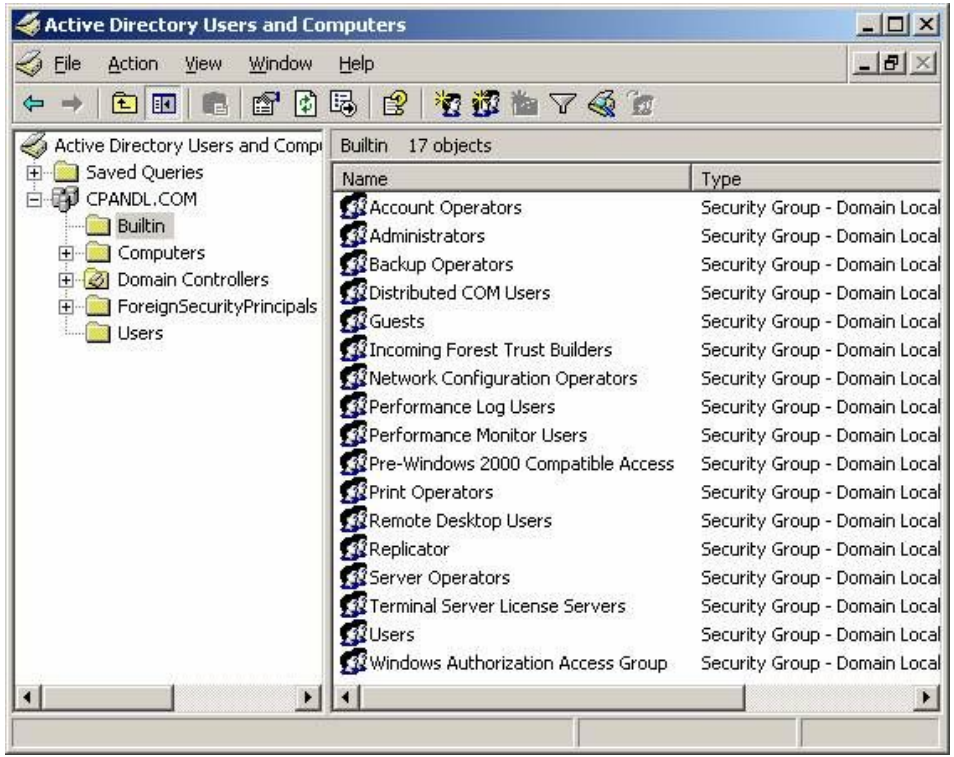
Danger Zone

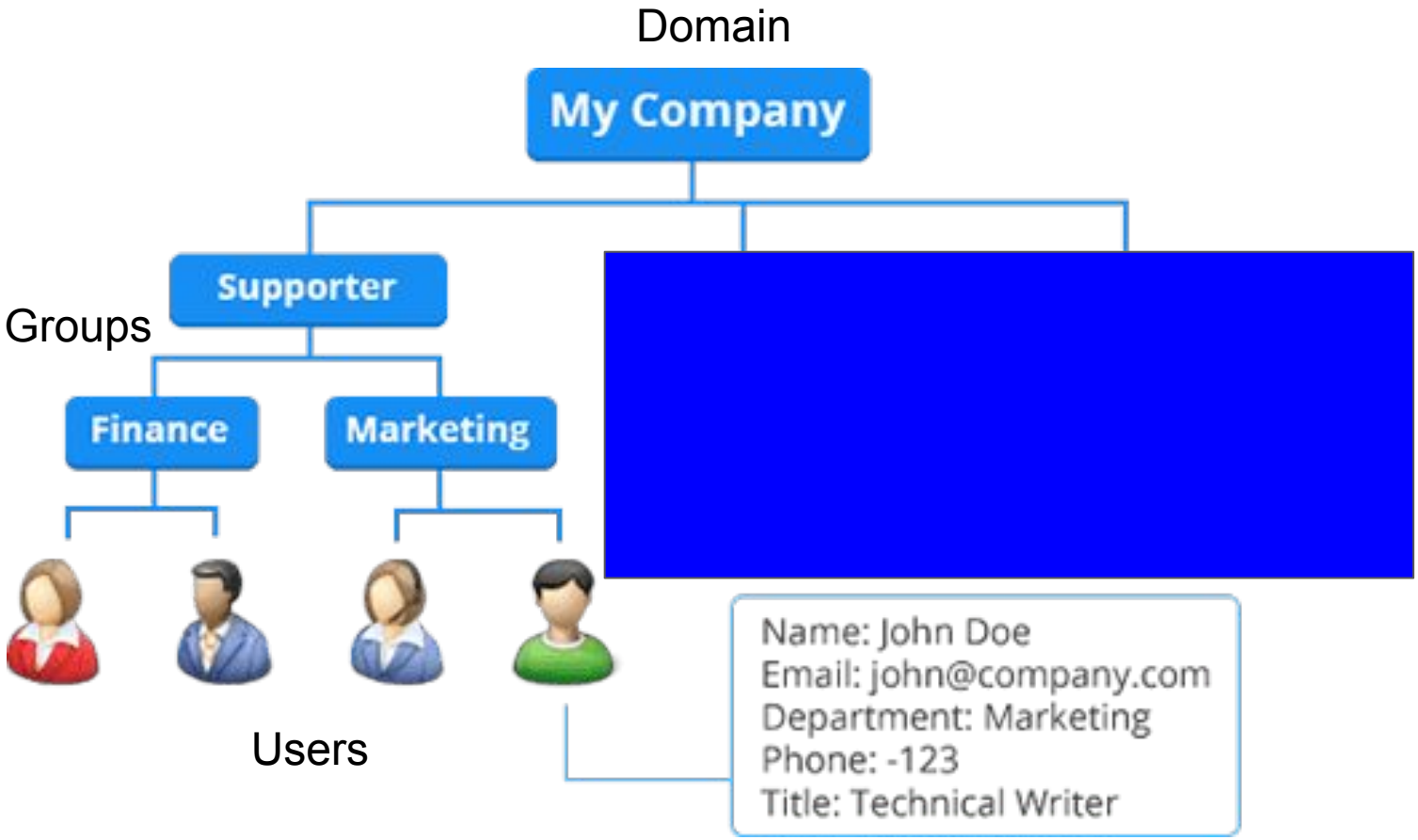
- Too many users to manage them all
  - UB has ~ 50,000 users
- Can leave security holes
  - Terminated employee
  - Other permission changes can affect
- Use groups instead



Security Groups

- Security groups are special folders inside Organizational Units (OU)
- Objects can be put in groups
- Helps keep organized
- Can assign settings to groups
- Acts similarly to users configuration
- Manage every user at once




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

Groups in Groups?

Nesting

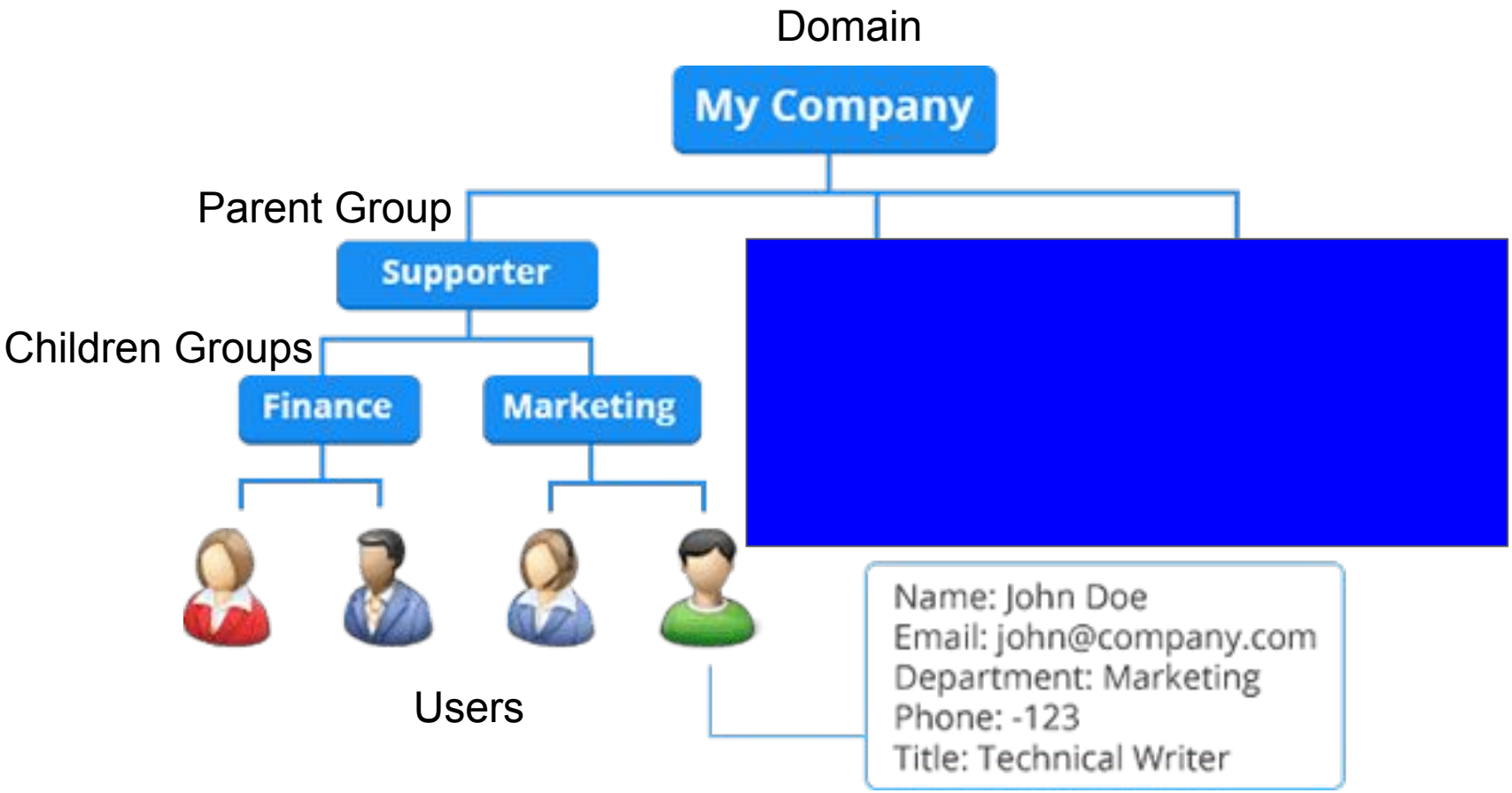
- Can put groups in groups
- Starts to get complicated
- Need to lay out organization before building AD
  - Build domain based on network layout and permissions
  - Does not always look the same as organization
- Leads to inheritance

Inheritance

Think of trickle down theory…..

- Sub groups (children objects) inherit permissions from group above (parent object)

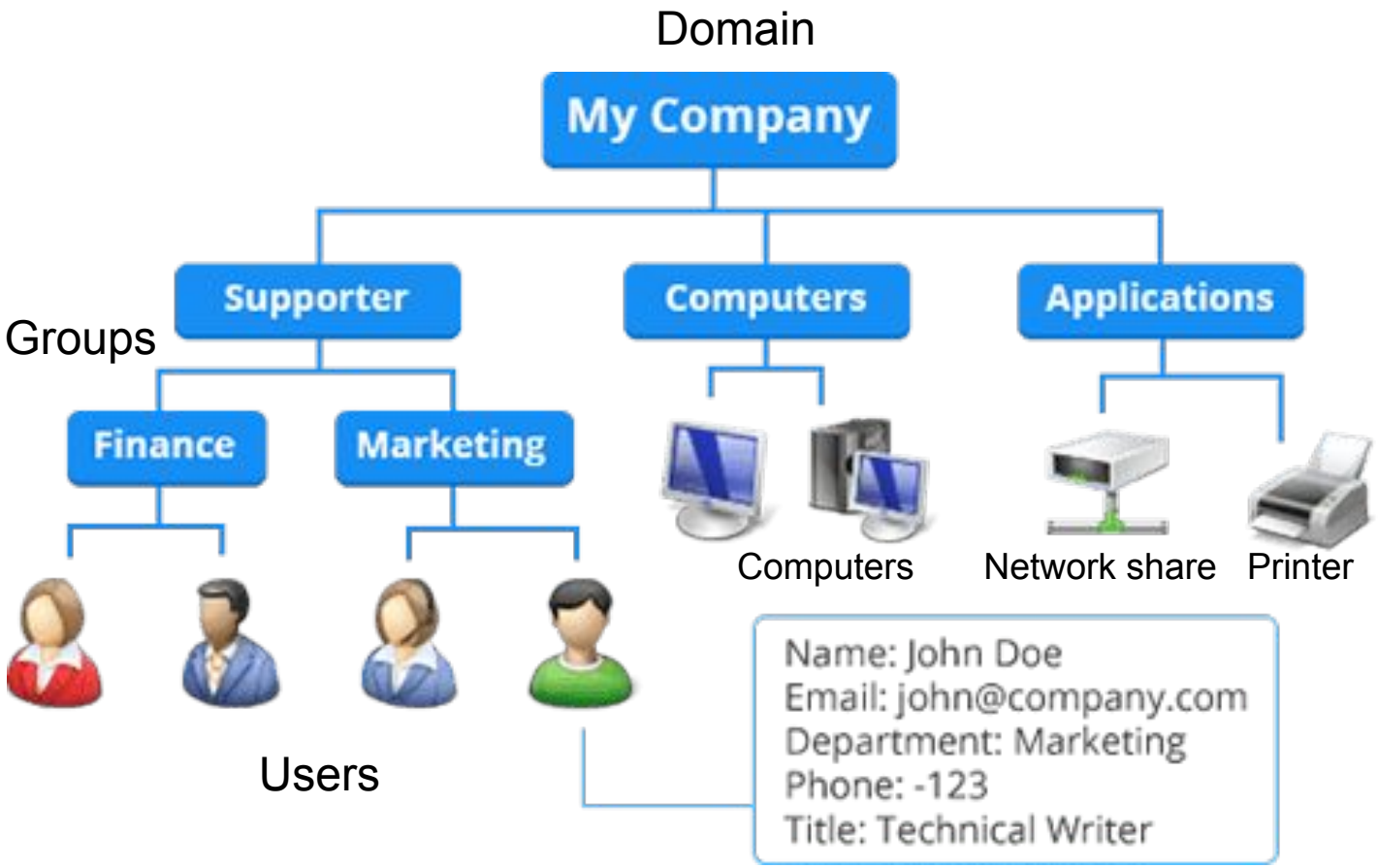
- Users in a group, in a group, will get settings placed on top level group

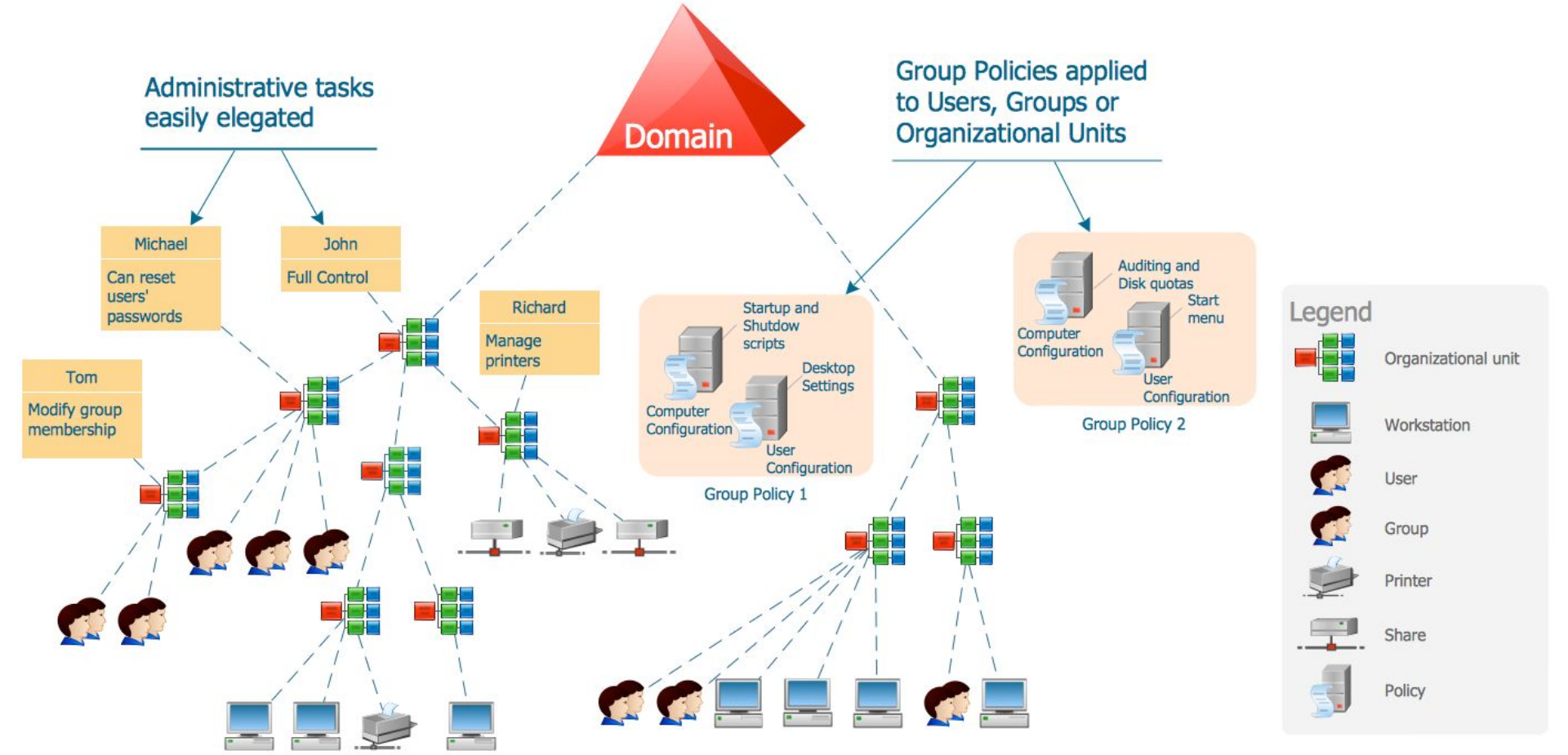

Domain
My Company
Parent Group
Supporter
Children Groups
Finance
Marketing
Users
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Computers and Devices

- Like users, devices can be managed in AD
- Computers
- Printers
- Other Servers

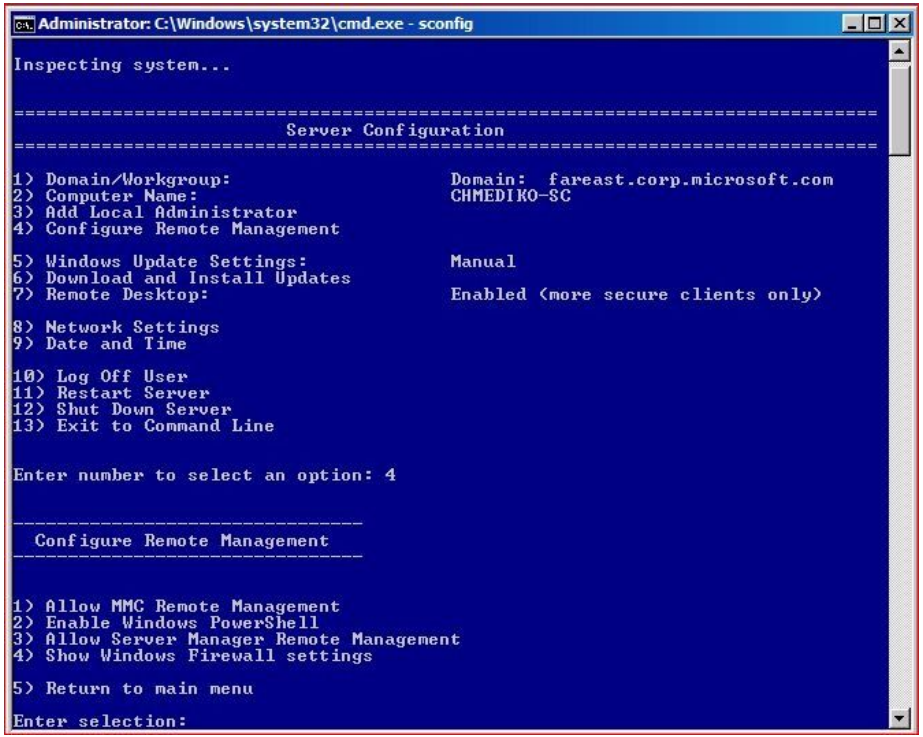
Can start to connect resources to each other


Domain
My Company
Groups
Supporter
Computers
Applications
Finance
Marketing
Computers
Network share
Printer
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer
Users


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
User
Group
Printer
Share
Policy

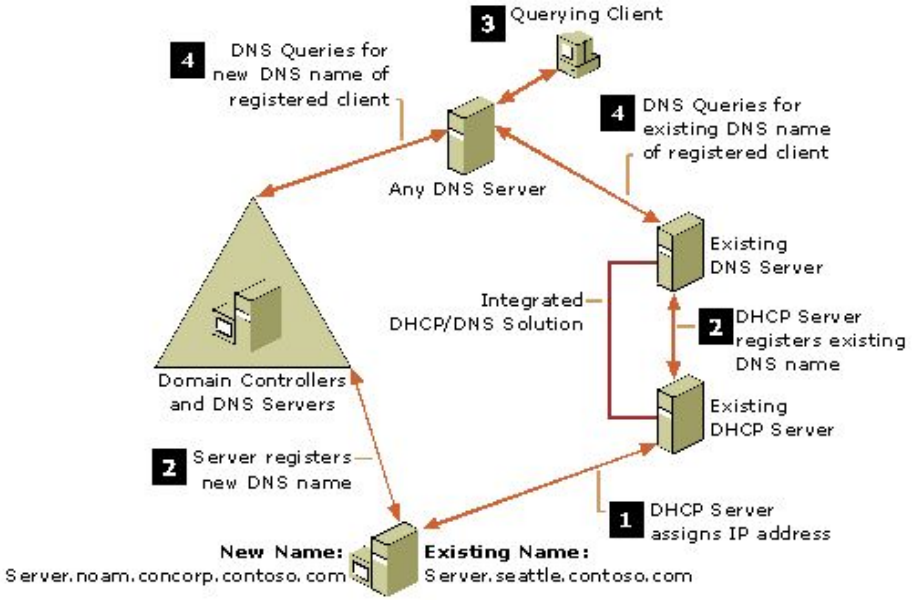
Confused yet?

- Domains control network
- OU’s store information about things (Objects)
- Security Groups also contain objects
- Groups can go in groups
- Children objects inherit permissions from parent objects

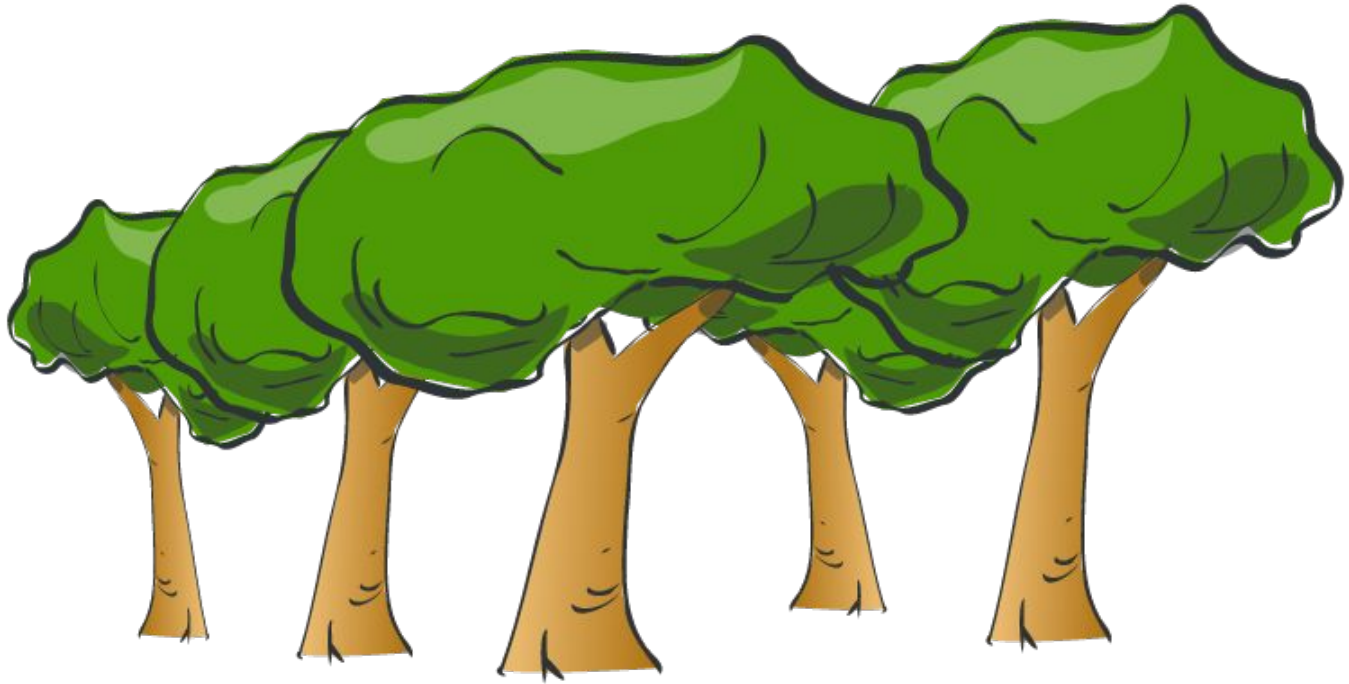


AD Tips

DON’T LET DNS DIE

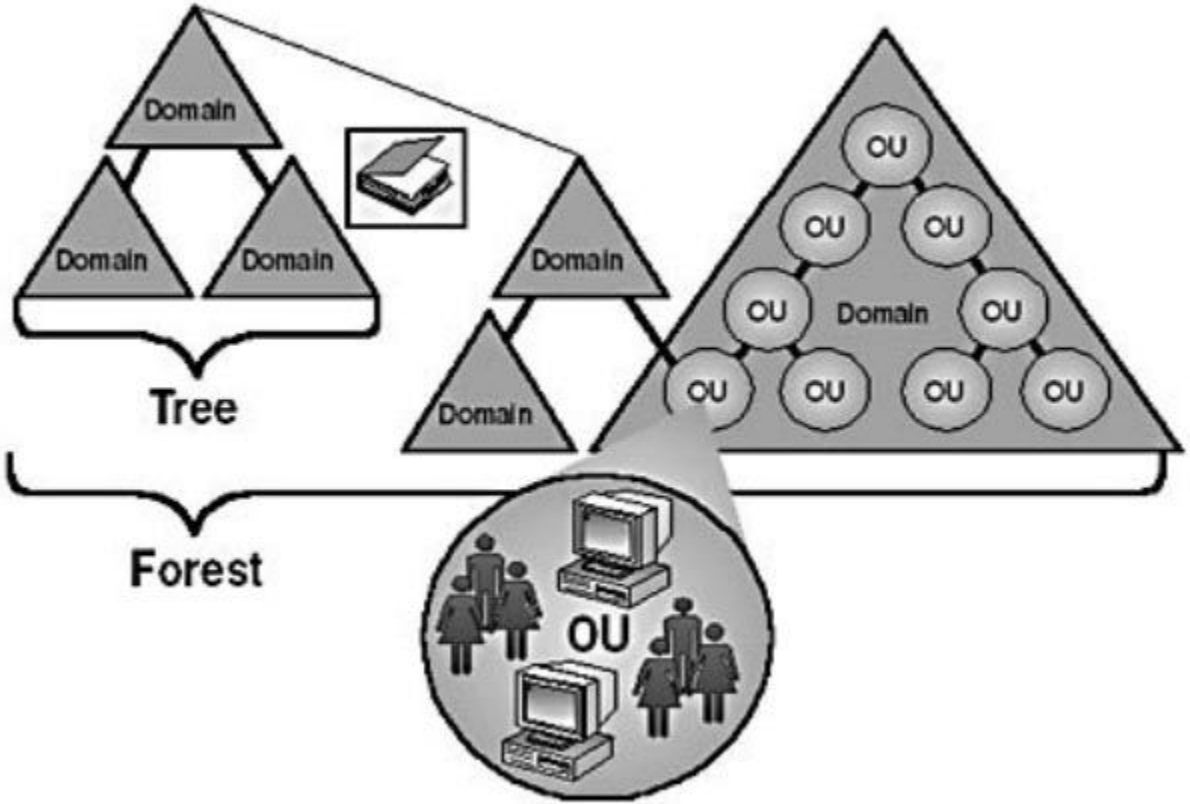


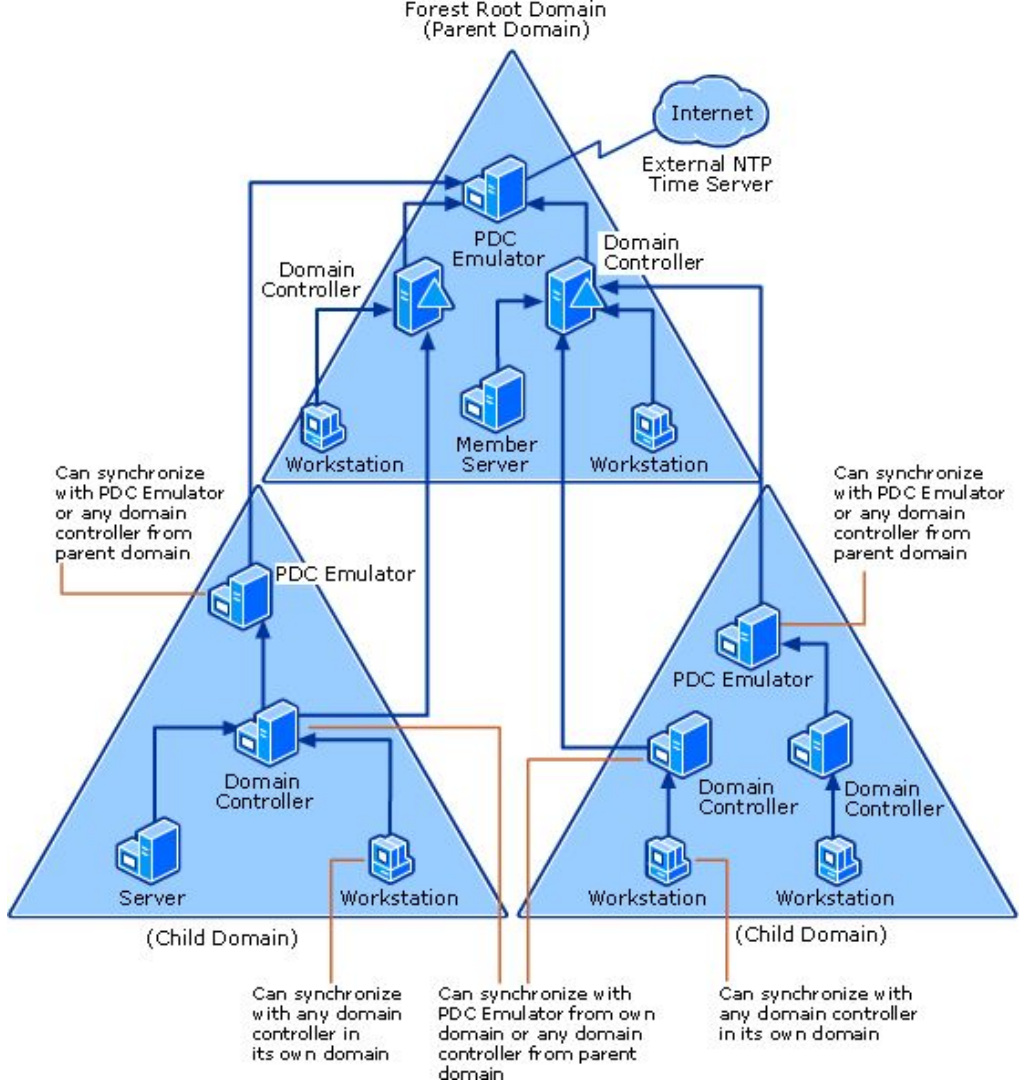
Forests, trees, and leaves



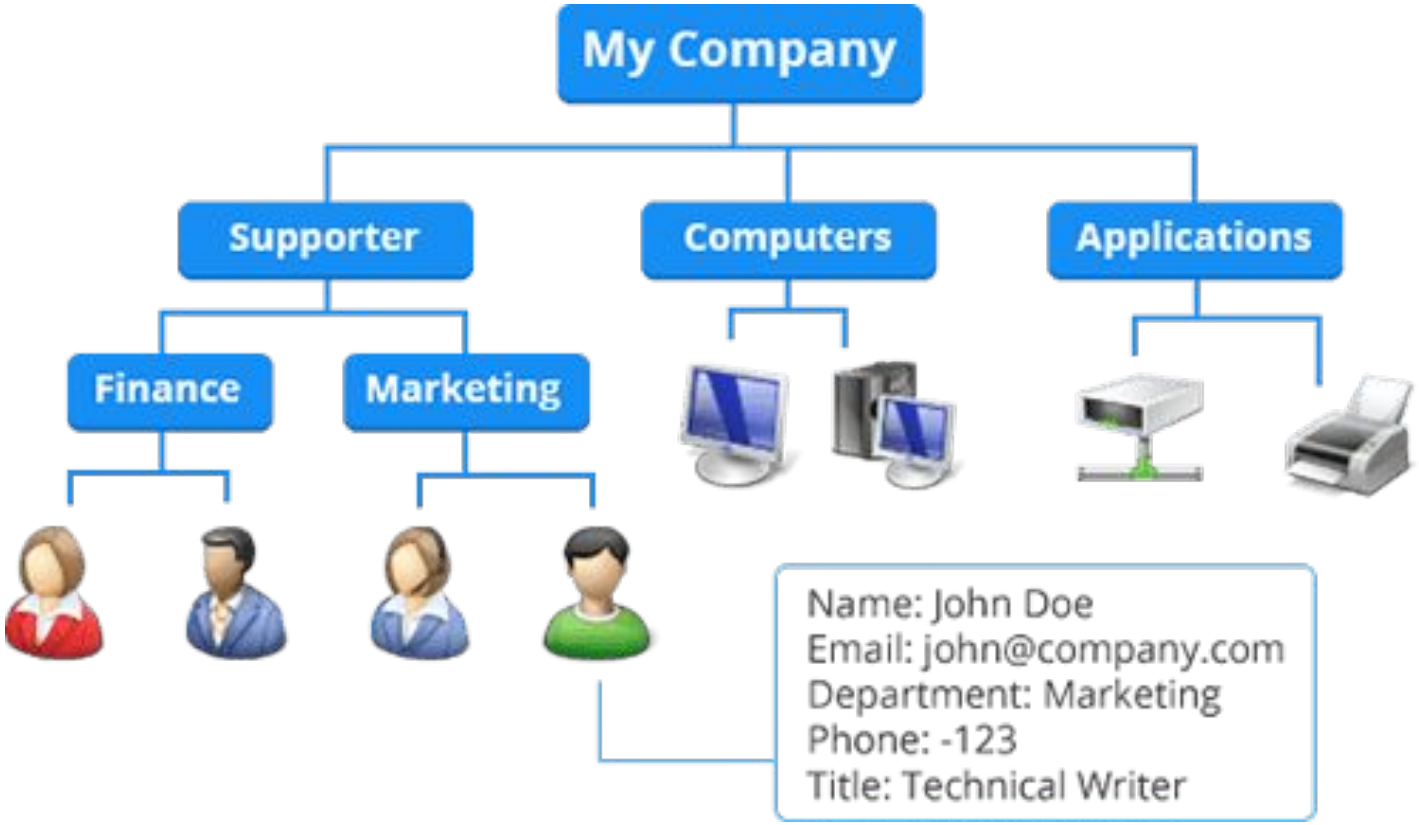
Forests, trees, and leaves

Forests, trees, and leaves



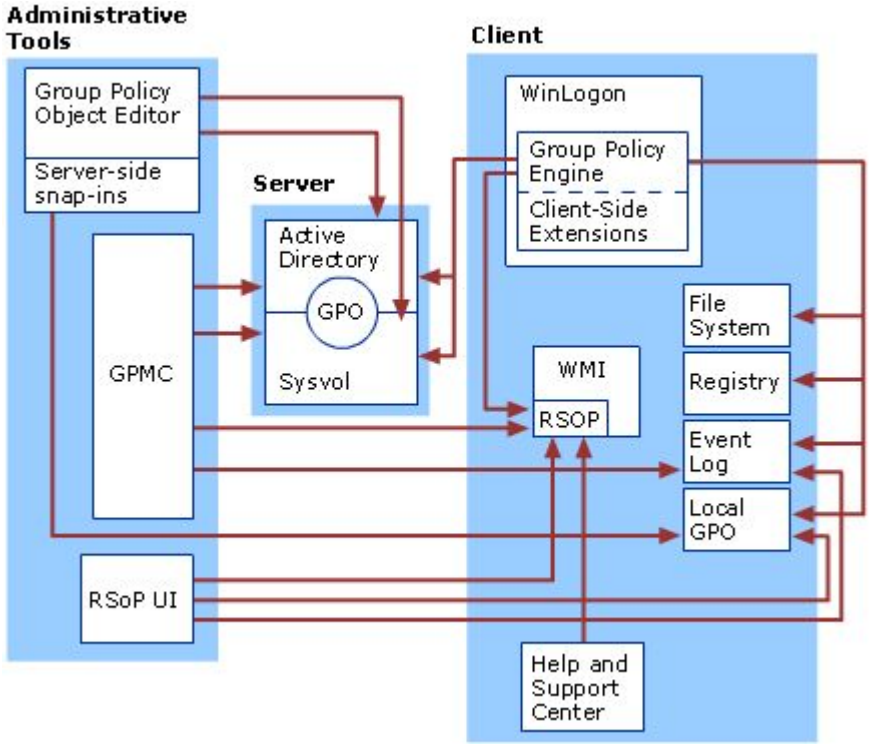

Forest Root Domain
(Parent Domain)
Internet
External NTP
Time Server
PDC
Emulator
Domain
Controller
Domain
Controller
Workstation
Member
Server
Workstation
Can synchronize
with PDC Emulator
or any domain
controller from
parent domain
PDC Emulator
Domain
Controller
Server
Workstation
(Child Domain)
Can synchronize
with any domain
controller in
its own domain
Can synchronize with
PDC Emulator from own
domain or any domain
controller from parent
domain
Can synchronize
with PDC Emulator
or any domain
controller from
parent domain
PDC Emulator
Domain
Controller
Domain
Controller
Workstation
Workstation
(Child Domain)
Can synchronize with
any domain controller
in its own domain

Active Directory



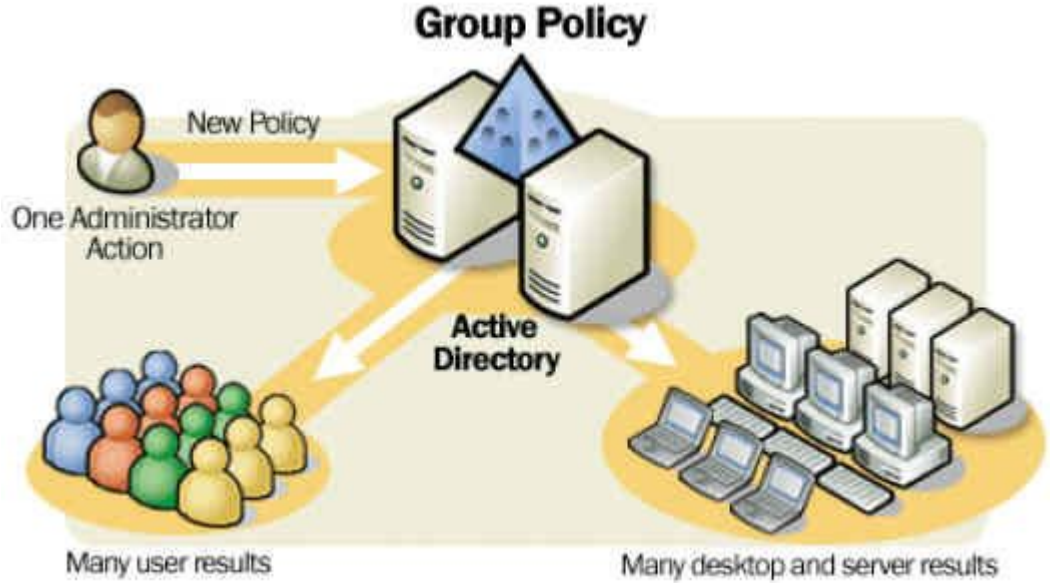
Group Policy

- Because this wasn't complicated enough already



Group Policy

- Centralized management tool for windows networks
- Can control pretty much every setting imaginable
- Works with Active Directory



For example…..

Mapped drives and folder redirection

Mapped Drives

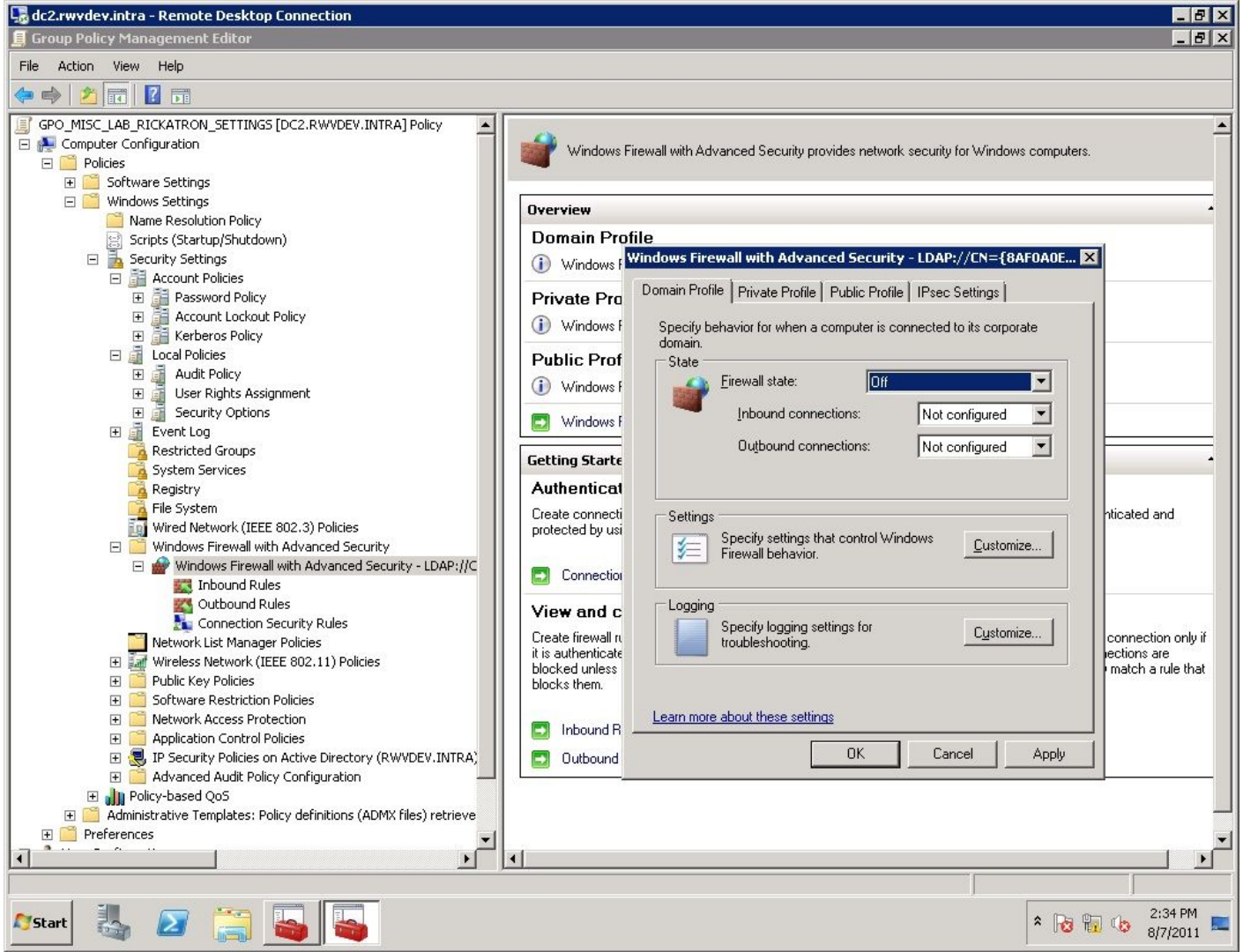
- Useful with many network drives
- Useful when user is moving computers
- Easy and seamless transition

Folder Redirection

- Nothing is stored locally
- Documents, pictures, desktop redirected to server
- Backups
- Mobility

Group Policy

- Can be used to force any setting on objects in AD
- Login scripts
- Mapped network drives
- Sleep settings
- Remote desktop access
- Password policy
- Set firewall policy
- Change background
- Change cursor
- Windows Update timing
- Pretty much anything you can think of


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

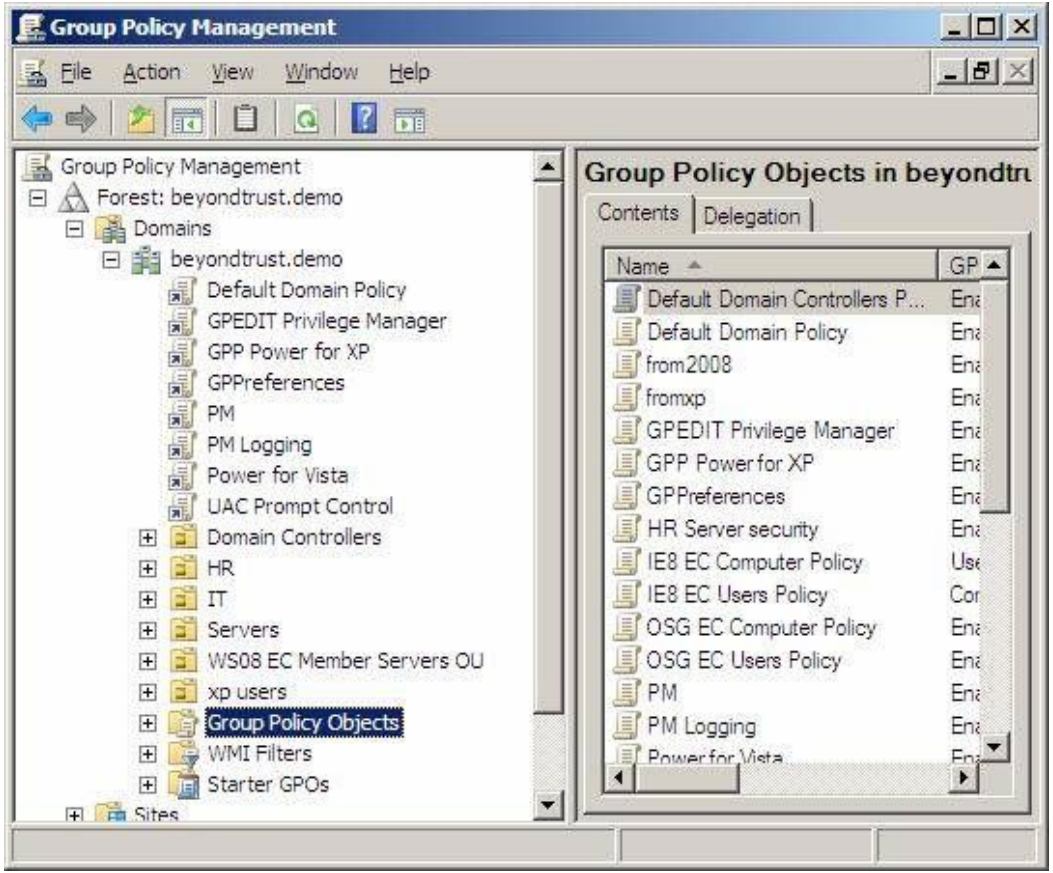
Group Policy

Key terms:

- Enforced
  - Can not be overwritten by other policy
- Linked
  - Link policy to specific OU
- Filtering
  - Can choose to apply Group policy to computers that meet criteria
  - < 4GB RAM
- Group Policy Object
  - A set of rules that can be applied to a network object

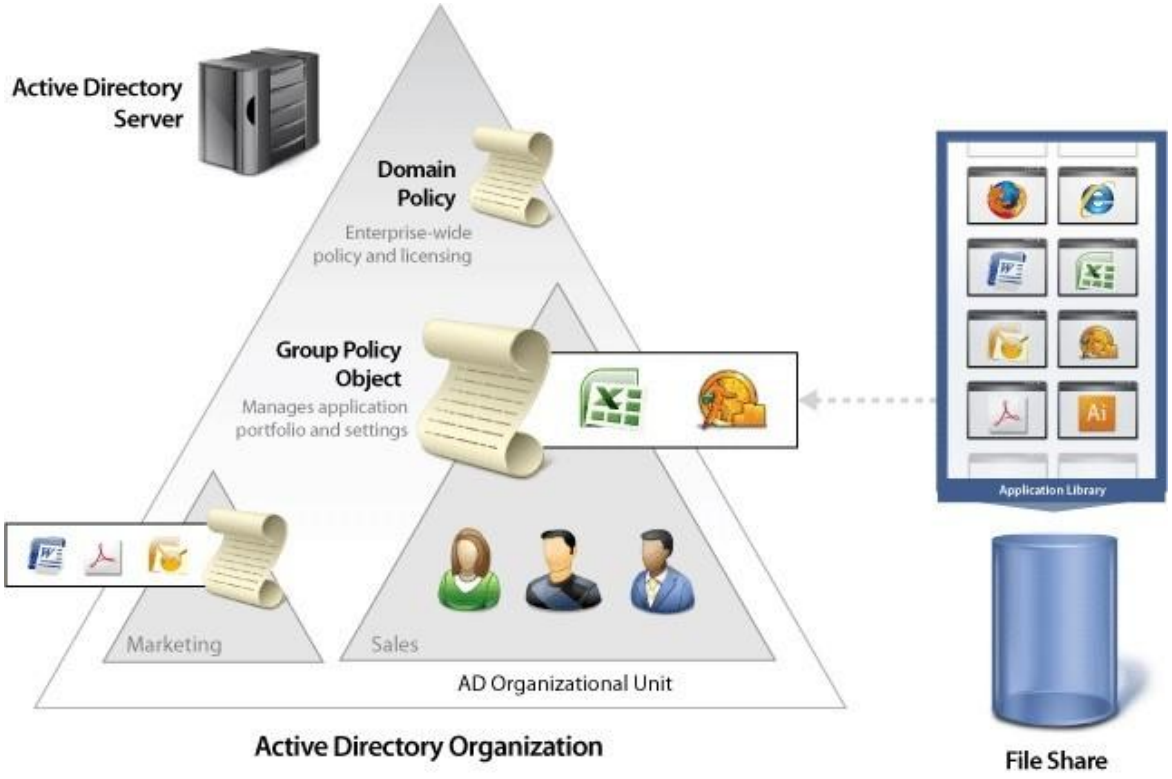
Multiple Group Policies

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



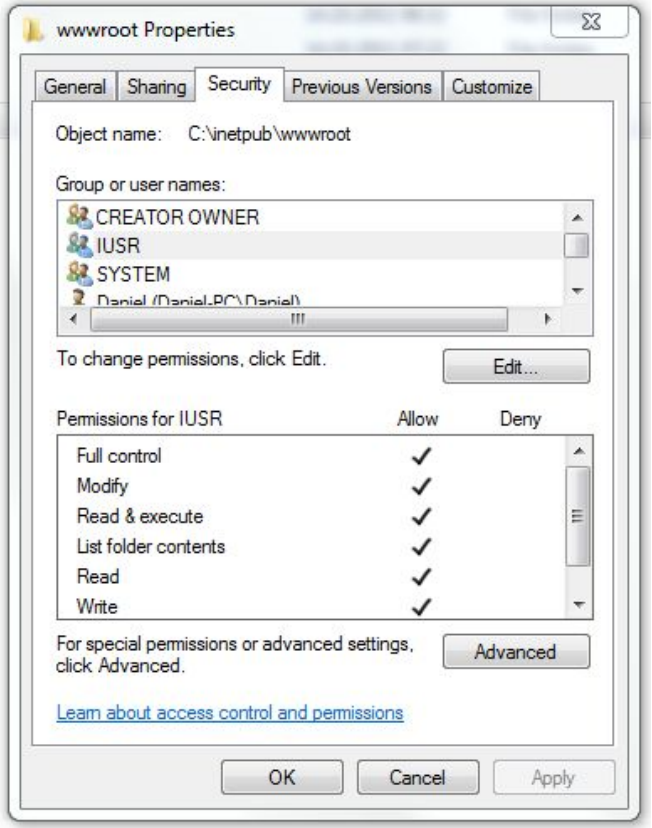
Active directory and Group Policy

- Some the the most powerful tools for an admin
- Can be used together to control 90% of functions
- Organization is key

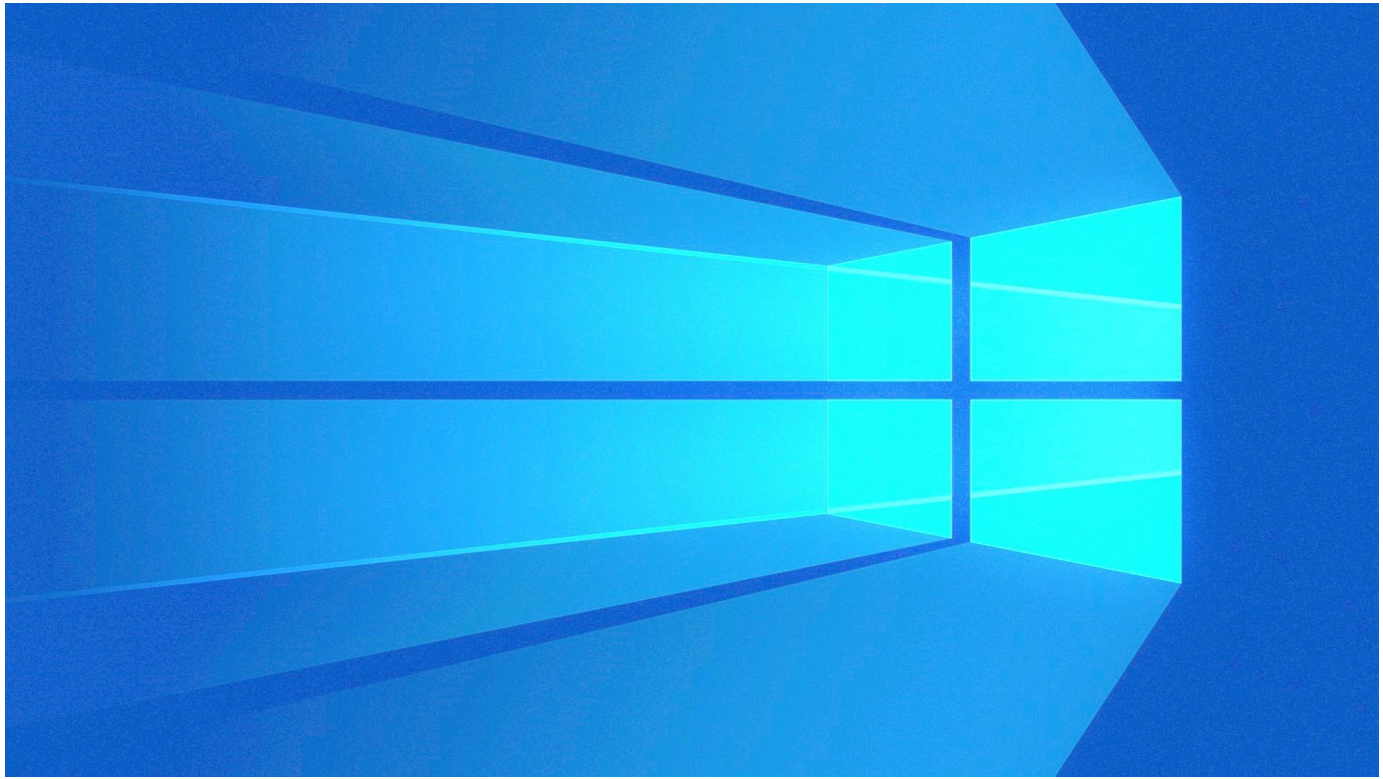


File Permissions

- 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

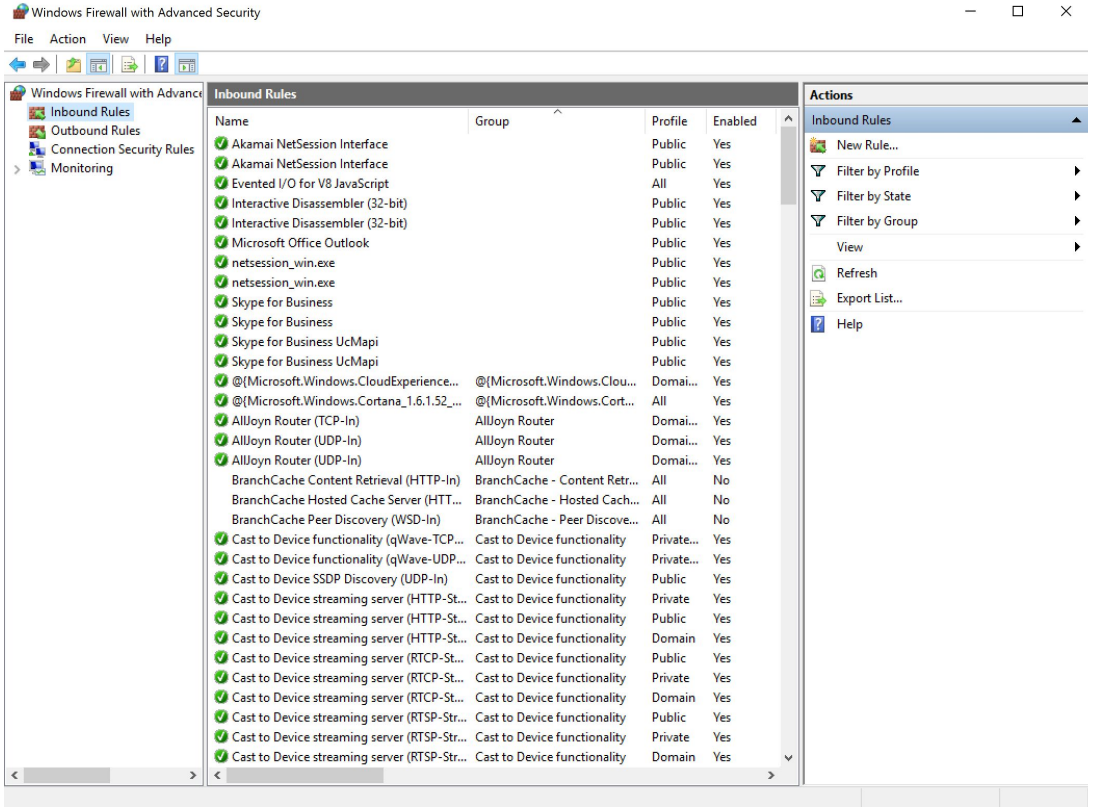


More Windows!



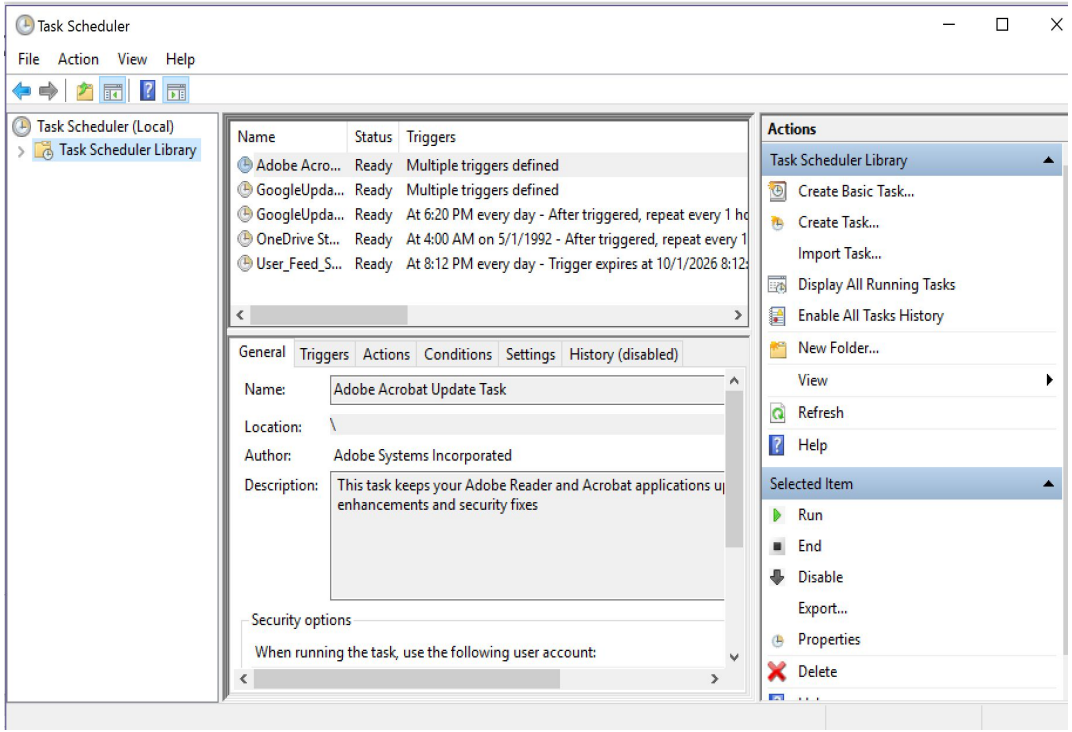
Windows Firewalls

- Does not act like Linux
- Order does not matter
- Can block specific EXE's, ports, or services
- Can specify which network to block on
  - Domain
  - Public
  - Private



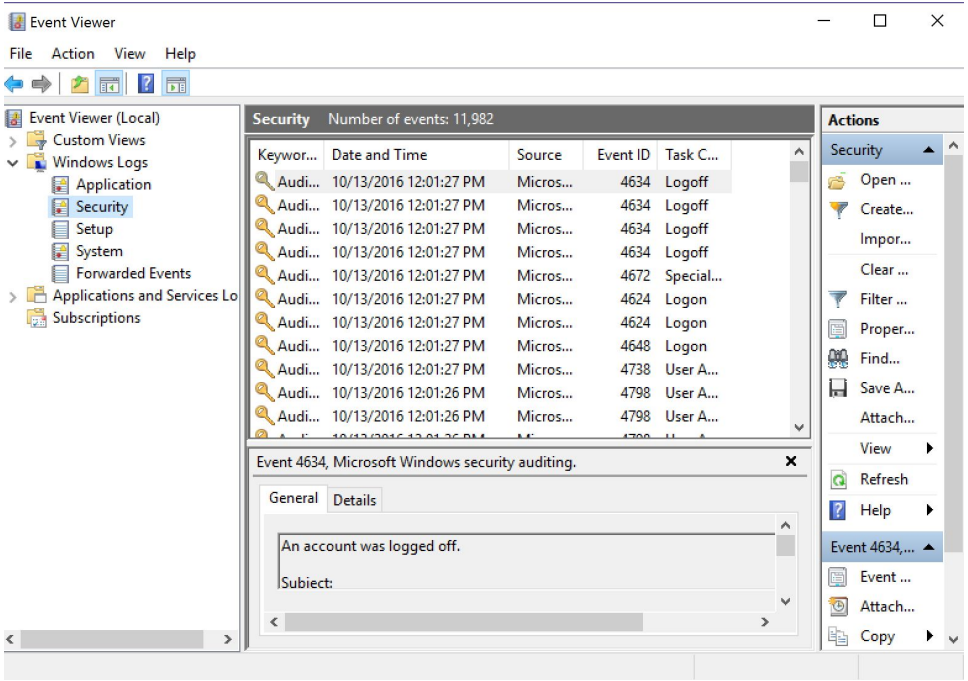
Task Scheduler

- Can be used to automate things
- Run at time intervals
- Run at specific events
- Run at startup
- Watch out for bad things, but use this for good things
- Use at work for backups



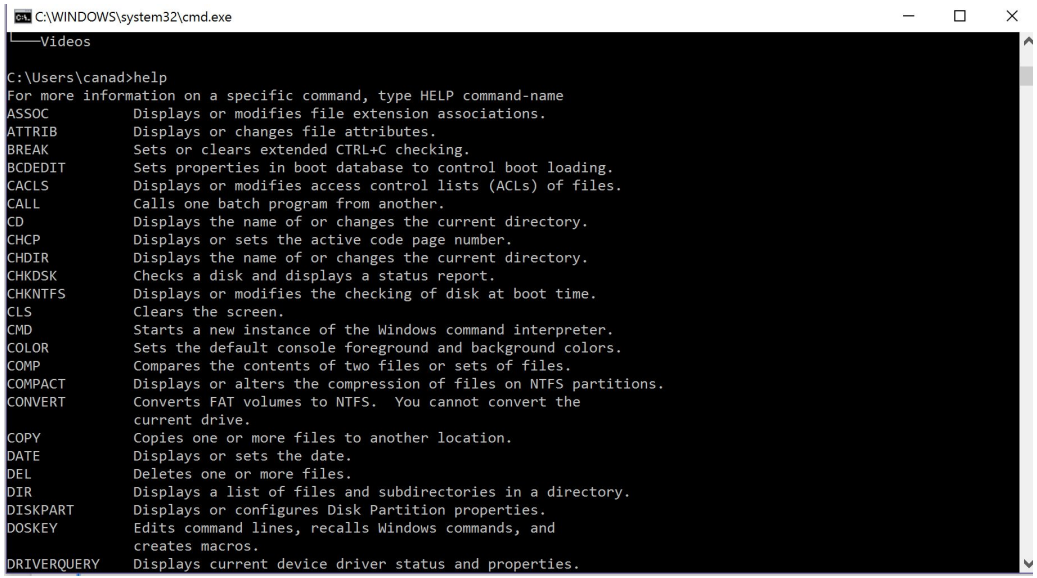
Event Viewer

- Monitors all system and application events
- Can be overwhelming
- Useful for troubleshooting
- Useful for looking for bad guys
- Centralized logging
  - Can send all logs to one server, aggregate data for analysis



Command line

- Basic windows commands
  - Ipconfig (Not Ifconfig!!!!)
  - Ping
  - Nslookup
  - Cd
  - Tracert
  - Tree
  - help



Powershell

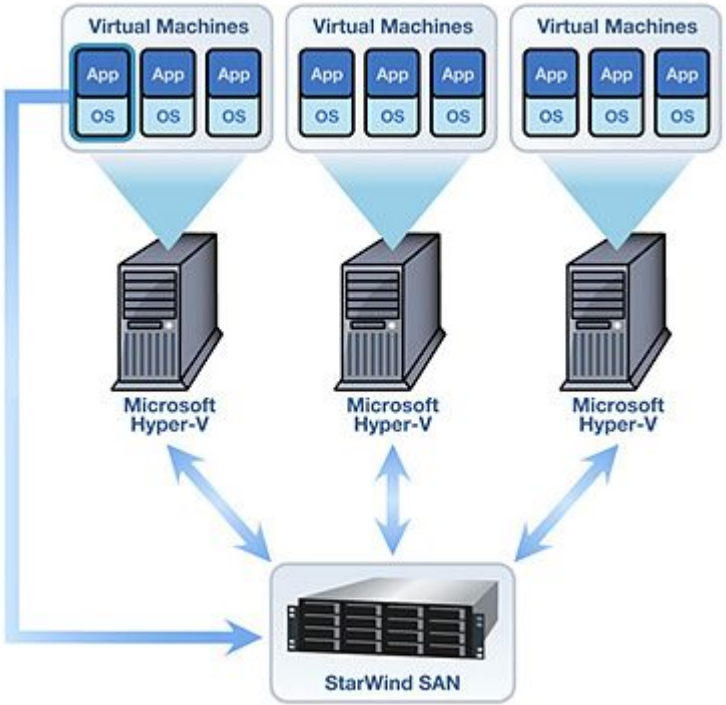
- Can do anything using powershell that you can do using GUI
- Just need to find the right commands
- Can create user and add them to group

```
Install-User -Username "User" -Description "LocalAdmin" -FullName "Local Admin by Powershell" -Password "Password01"
Add-GroupMember -Name 'Administrators' -Member 'User'
```

- Google is your friend

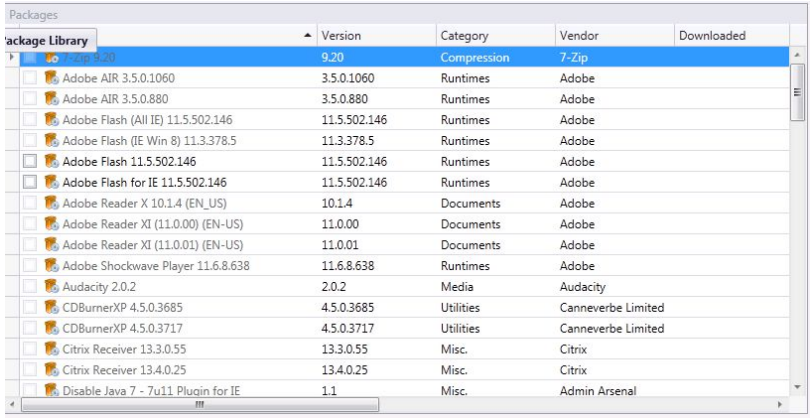
Virtualization

- Hyper-V is windows hypervisor
- Useful for segmentation of services
- Backup DC- probably don't want to virtualize



Windows Admin Tools

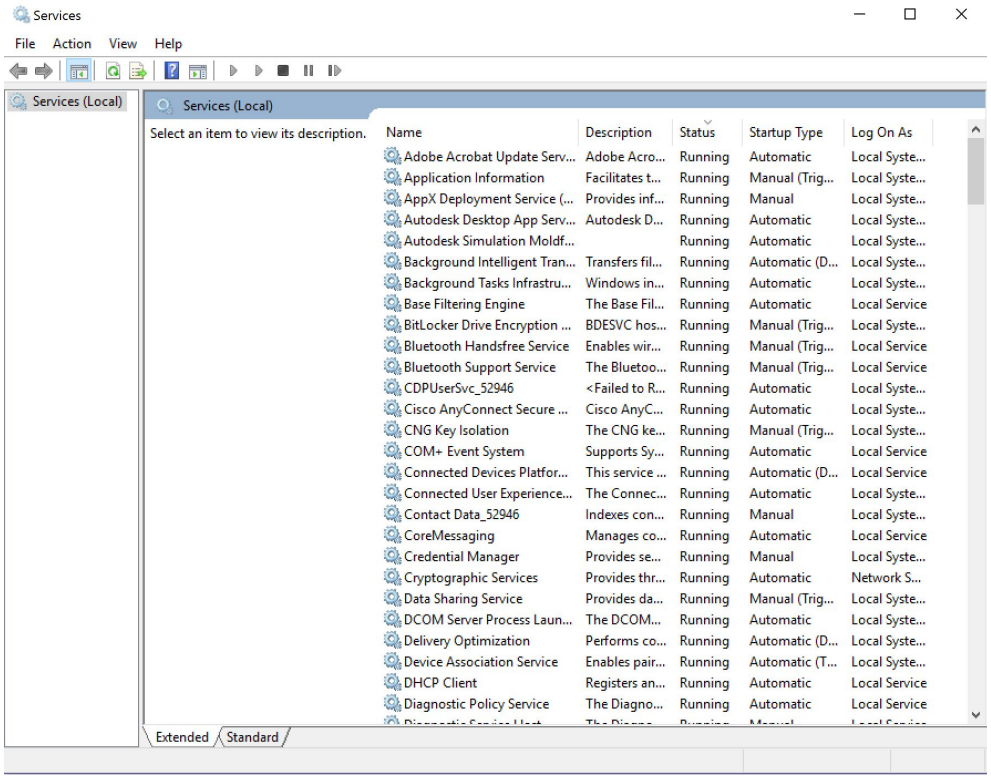
- View open folders and files
  - Can be useful for troubleshooting a locked file
  - Can be useful for keeping attackers out
- Storage spaces
  - Software raid
- WSUS
  - Centralized windows updates
- Application deployment
  - PDQ deploy
  - Uses powershell to push out applications
- Process explorer
  - Dive deeper into whats running

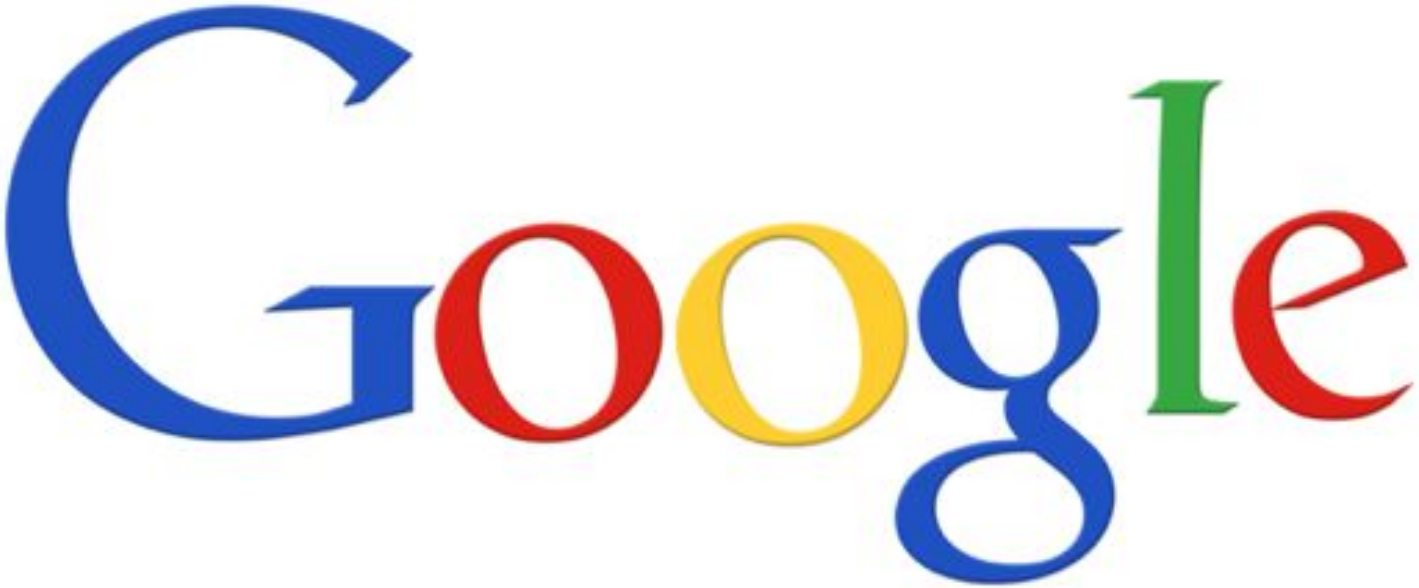


Windows Services (not roles and features)

- Are simply long running processes managed by the Windows Service Manager

- Windows services have 5 different states: Start,Stop, Pause, Resume, and Restart




Google