

Windows

Not just for houses

Windows 1-10



Windows Server

Essentially a jacked up windows 8 box

- Still GUI based
- Still makes no sense
- No start menu :(ul>- (Install classic shell)... trust me...



Windows Server

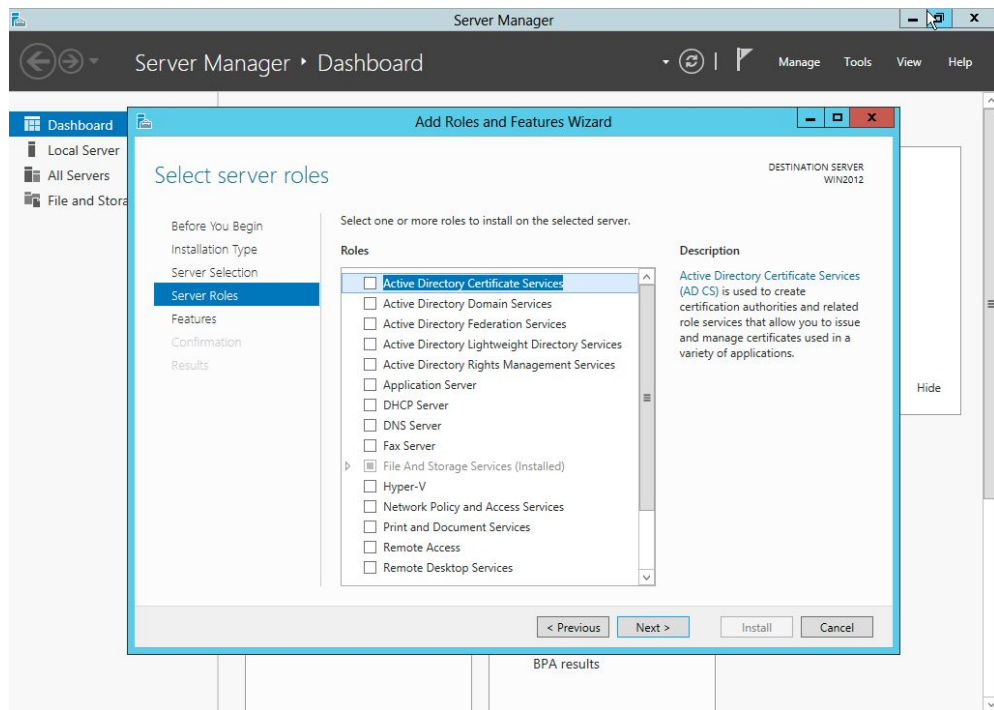
What can it do?

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



Roles and Features

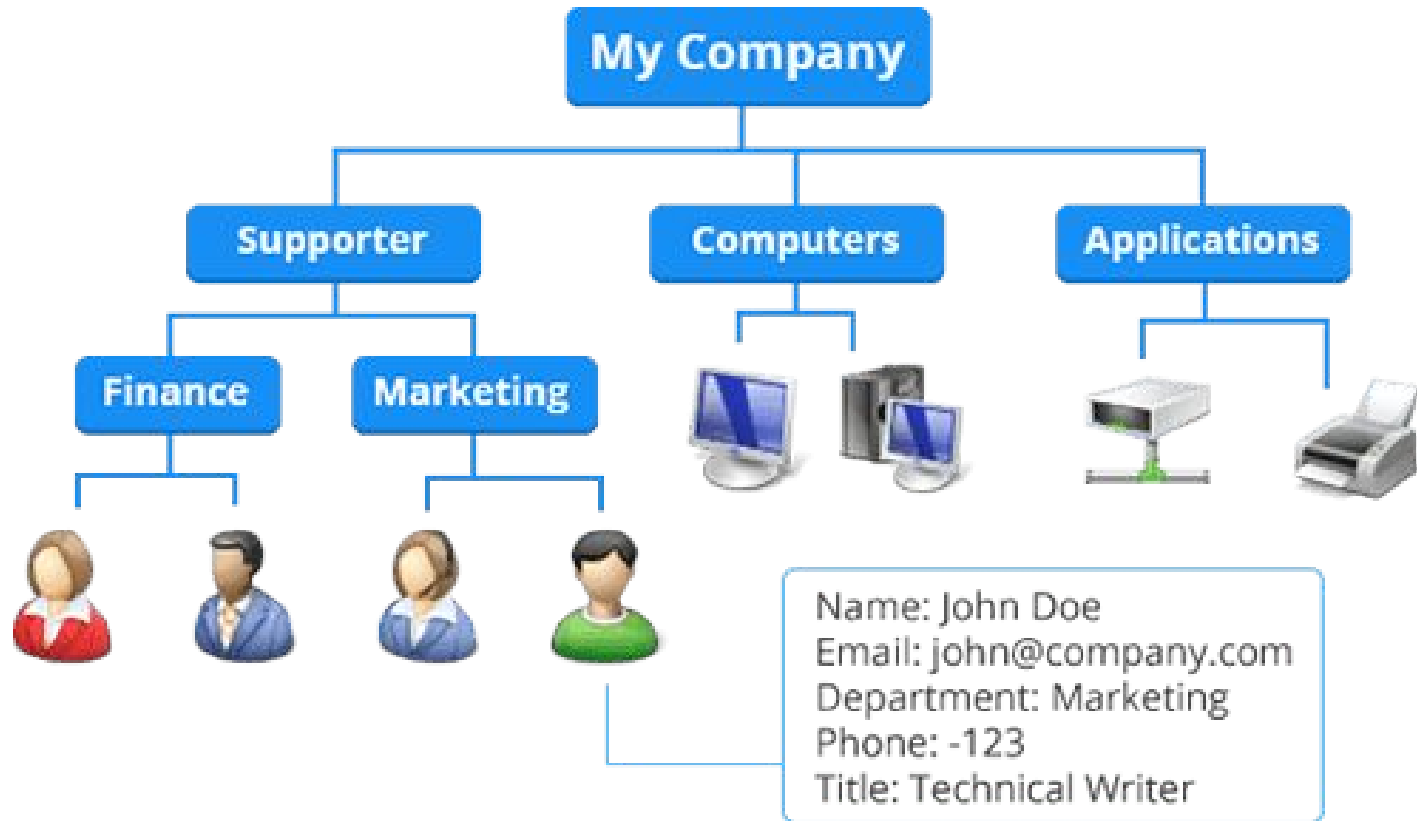
Building blocks for everything Windows server



Common Roles and Features

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

Active Directory

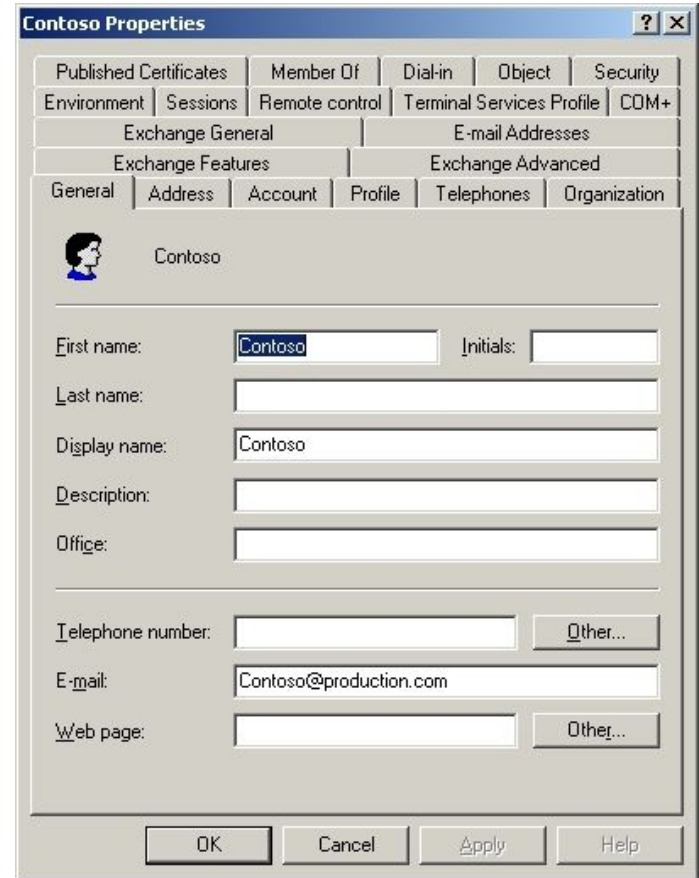


Active Directory

- Database of objects in a network (Domain)
 - Users
 - Computers
 - Printers
 - more
- Stores objects in hierarchy
 - Called organizational units (OU)
 - Duplicate real world hierarchy of organization

Users

- Stores information on user
 - 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 has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with the following tabs: Published Certificates, Member Of, Dial-in, Object, Security, Environment, Sessions, Remote control, Terminal Services Profile, COM+, Exchange General, E-mail Addresses, Exchange Features, Exchange Advanced, General, Address, Account, Profile, Telephones, and Organization. The 'General' tab is active, showing a user icon and the name 'Contoso'. Below this, there are several text input fields: 'First name:' (containing 'Contoso'), 'Initials:' (empty), 'Last name:' (empty), 'Display name:' (containing 'Contoso'), 'Description:' (empty), 'Office:' (empty), 'Telephone number:' (empty), 'E-mail:' (containing 'Contoso@production.com'), and 'Web page:' (empty). There are also buttons for 'Other...' next to the 'Telephone number' and 'Web page' fields. At the bottom of the dialog box are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

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

The screenshot shows the 'Contoso Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and close button. Below the title bar is a tabbed interface with the following tabs: Published Certificates, Member Of, Dial-in, Object, Security, Environment, Sessions, Remote control, Terminal Services Profile, COM+, Exchange General, E-mail Addresses, Exchange Features, Exchange Advanced, General, Address, Account, Profile, Telephones, and Organization. The 'General' tab is active, showing a user icon and the name 'Contoso'. Below this are several text input fields: 'First name:' with 'Contoso', 'Initials:', 'Last name:', 'Display name:' with 'Contoso', 'Description:', 'Office:', 'Telephone number:', 'E-mail:' with 'Contoso@production.com', and 'Web page:'. There are 'Other...' buttons next to the 'Telephone number' and 'Web page' fields. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Mapped drives and folder redirection

Mapped Drives

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

Folder Redirection

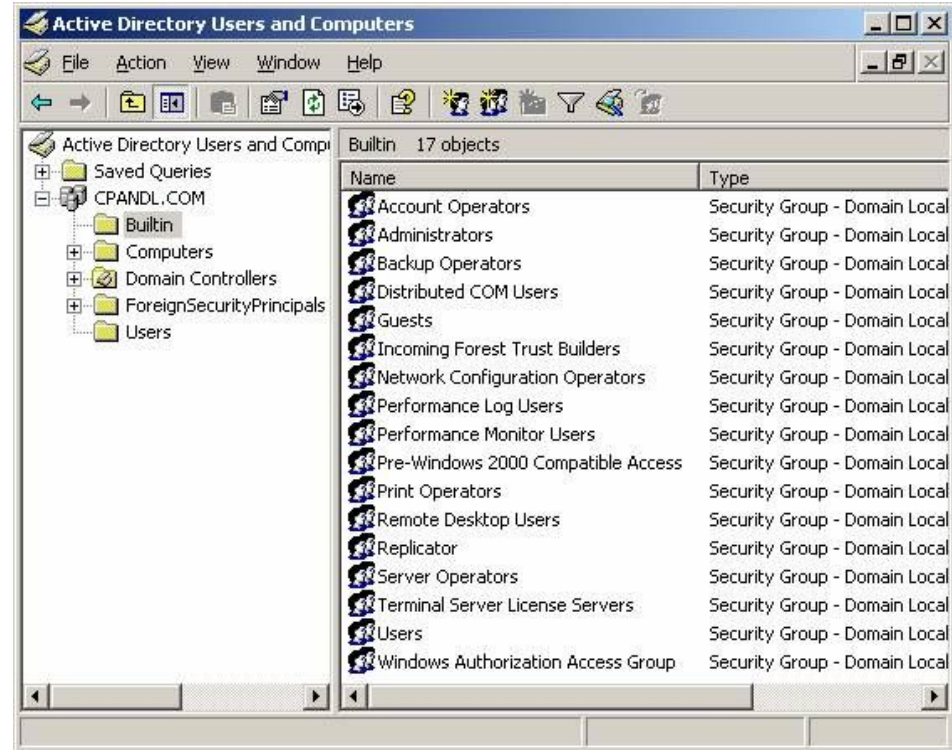
- Nothing is stored locally
- Documents, pictures, desktop redirected to server
- Backups
- Mobility

Why this is bad

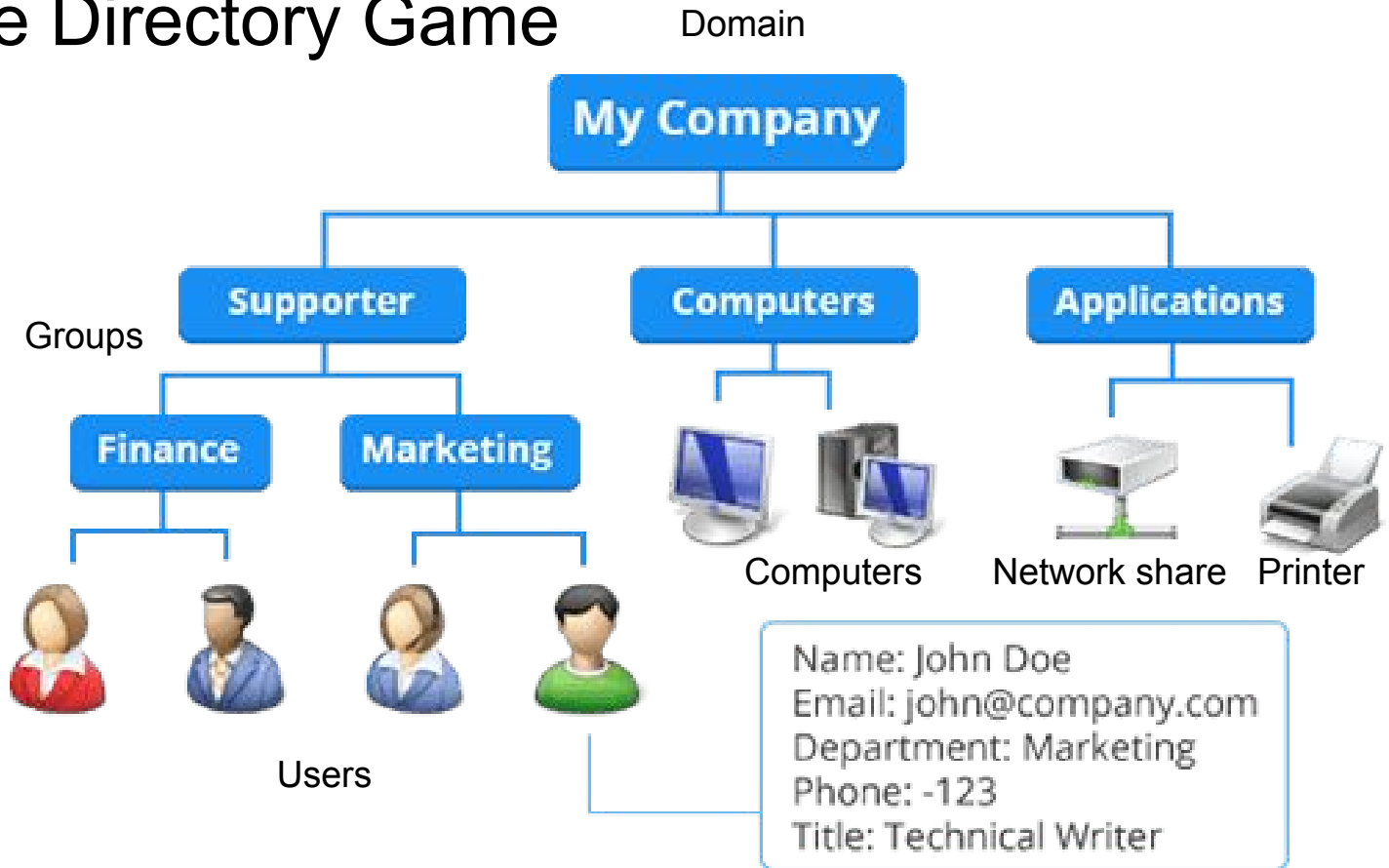
- Too many users to manage them all
 - UB has ~ 30,000 users
- Can leave security holes
 - Terminated employee
 - Other permission changes can affect
- Use groups instead

Groups

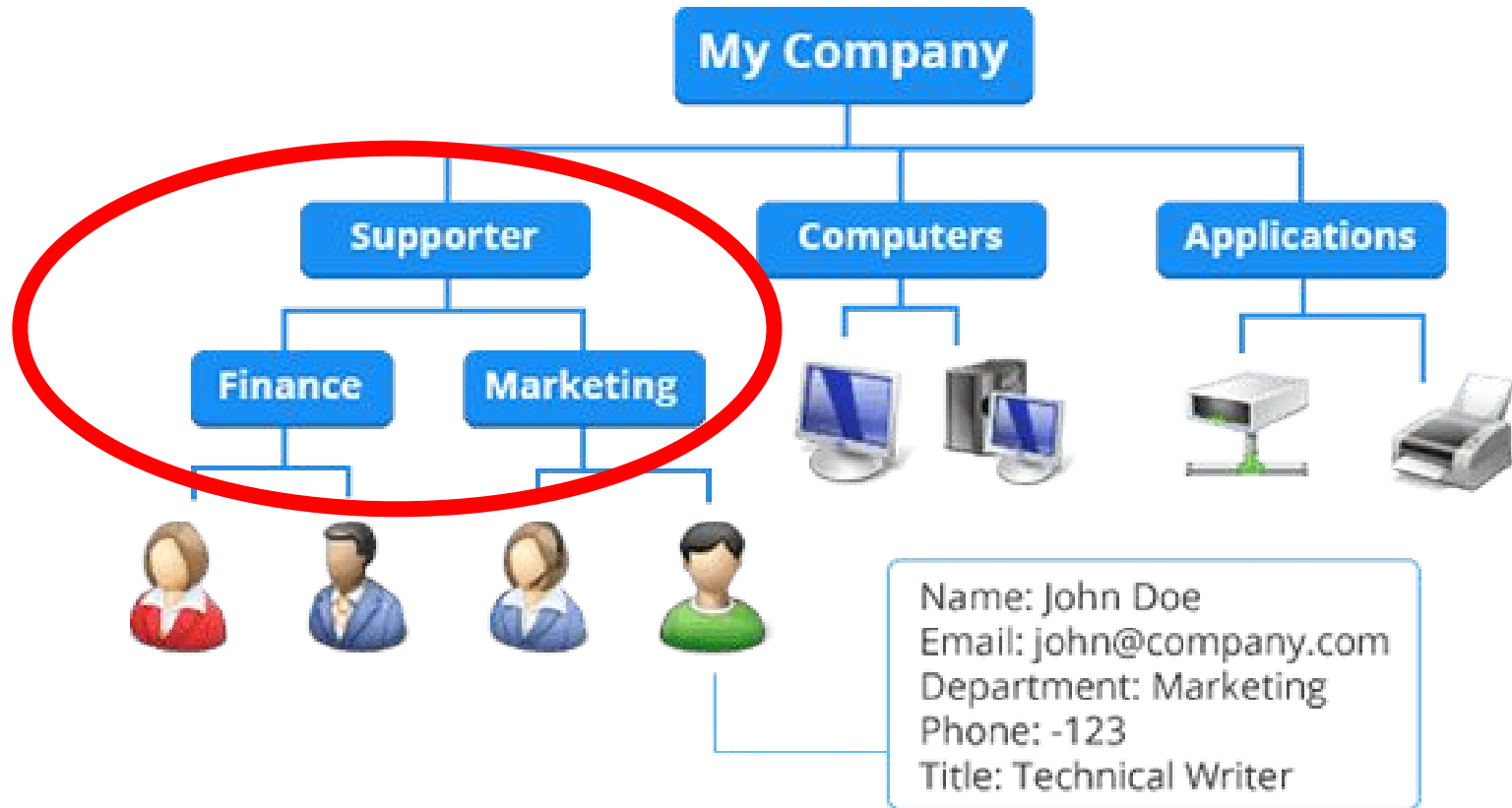
- Objects can be put in groups
- Helps keep organized
- Can assign settings to groups
- Acts similarly to users configuration
- Manage every user at once



Active Directory Game



Groups in Groups?



Nesting

- Can put groups in groups
- Starts to get complicated
- Need to lay out organization before building AD
- Leads to inheritance

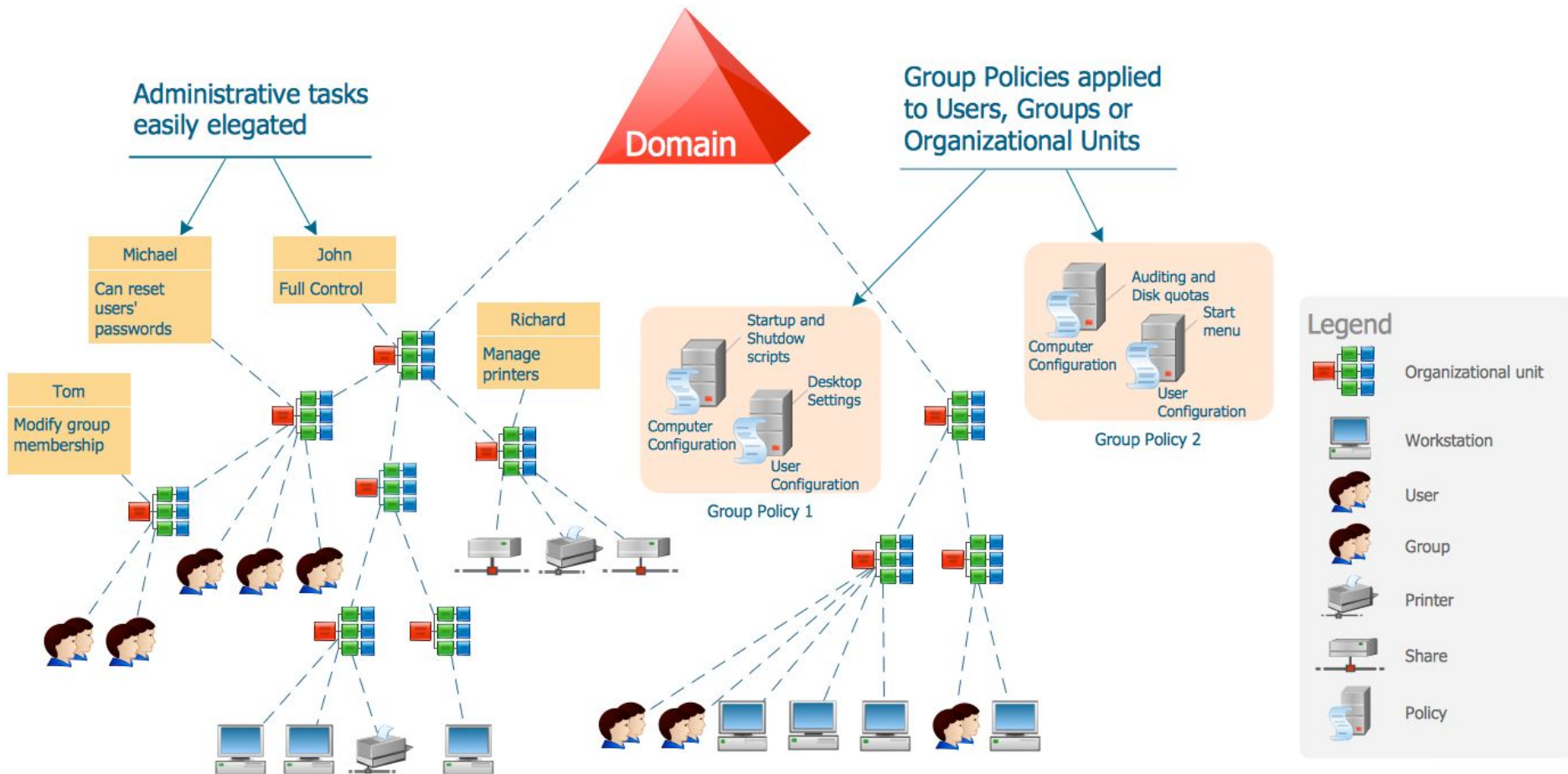


Inheritance

Think of trickle down theory..... But if it actually worked

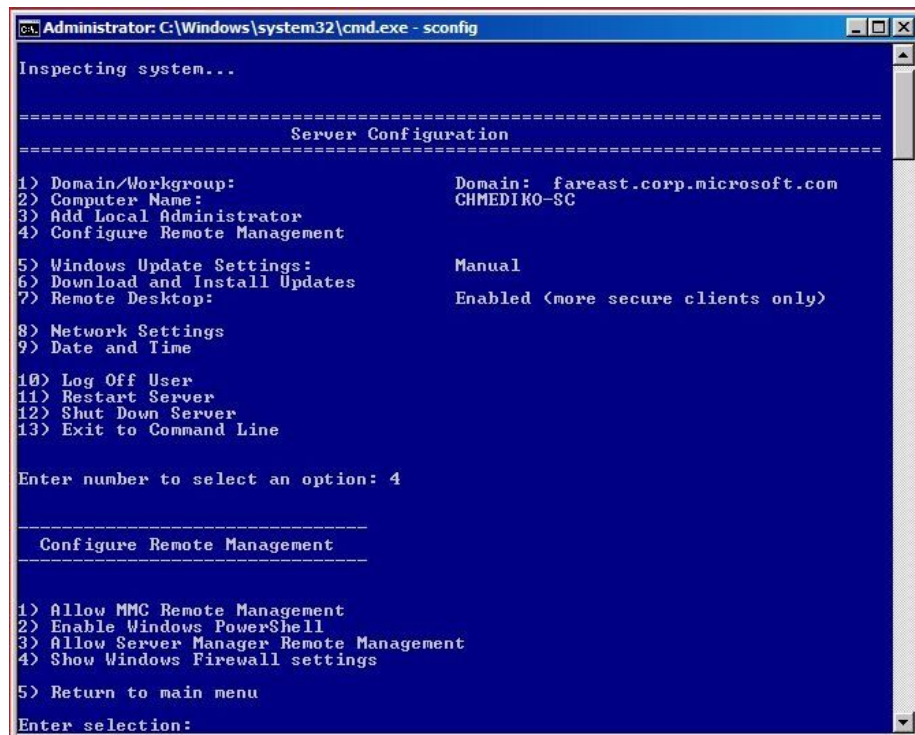
- Sub groups inherit permissions from group above
- Users in a group, in a group, will get settings placed on top level group





Confused yet?

- Domains control network
- OU's store information on things (objects)
- Groups contain objects
- Groups go in groups
- Windows is GUI (unless it's not) :(



```
Administrator: C:\Windows\system32\cmd.exe - sconfig

Inspecting system...

=====
                          Server Configuration
=====

1> Domain/Workgroup:                Domain:  fareast.corp.microsoft.com
2> Computer Name:                   CHMEDIKO-SC
3> Add Local Administrator
4> Configure Remote Management

5> Windows Update Settings:         Manual
6> Download and Install Updates
7> Remote Desktop:                   Enabled (more secure clients only)

8> Network Settings
9> Date and Time

10> Log Off User
11> Restart Server
12> Shut Down Server
13> Exit to Command Line

Enter number to select an option: 4

-----
          Configure Remote Management
-----

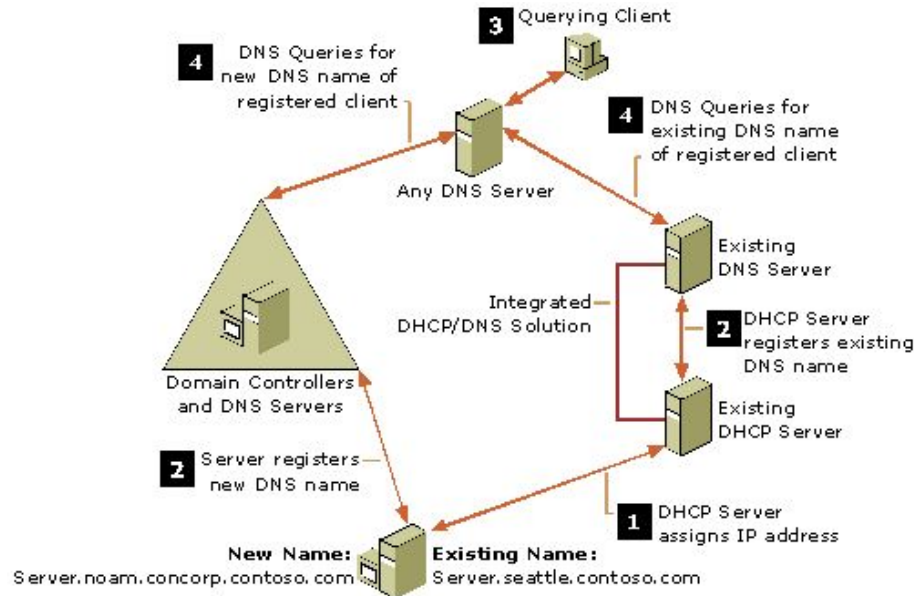
1> Allow MMC Remote Management
2> Enable Windows PowerShell
3> Allow Server Manager Remote Management
4> Show Windows Firewall settings

5> Return to main menu

Enter selection:
```

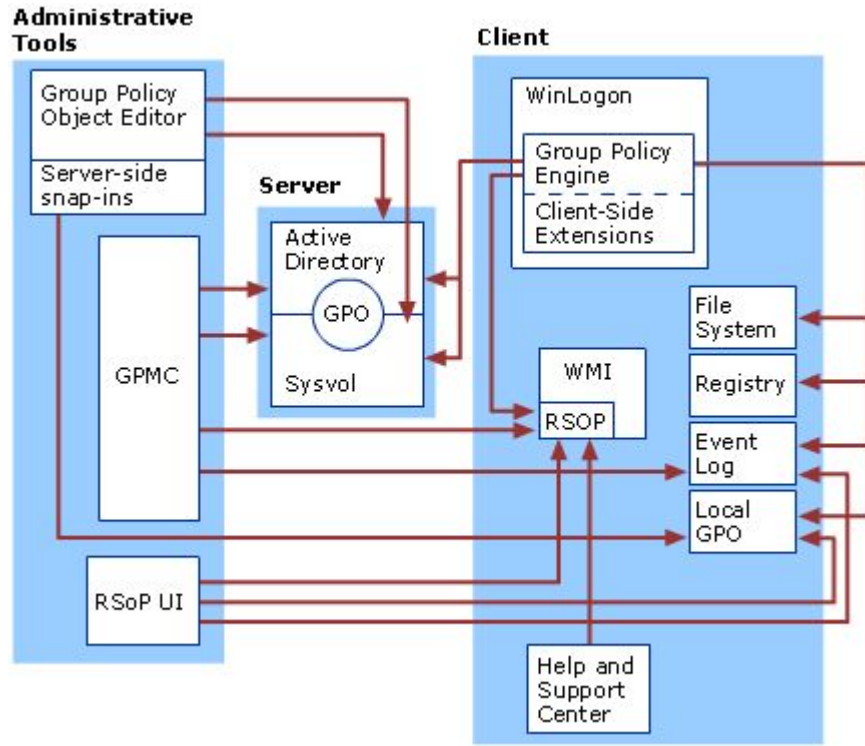
AD Tips

DON'T LET DNS DIE



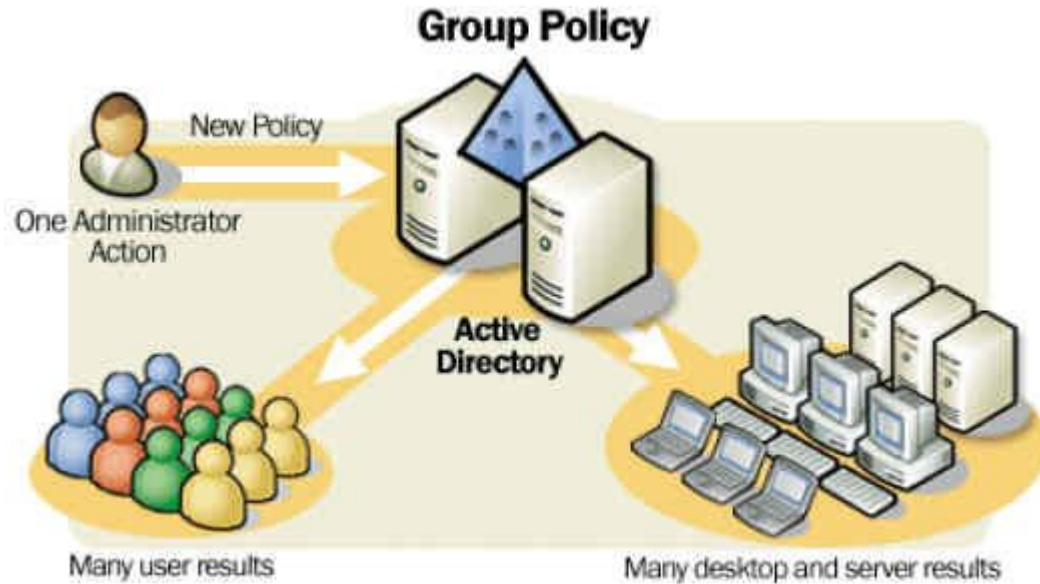
Group Policy

- Because this wasn't complicated enough already



Group Policy

- Centralized management tool for windows networks
- Can control machine level setting
- Works with Active Directory



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



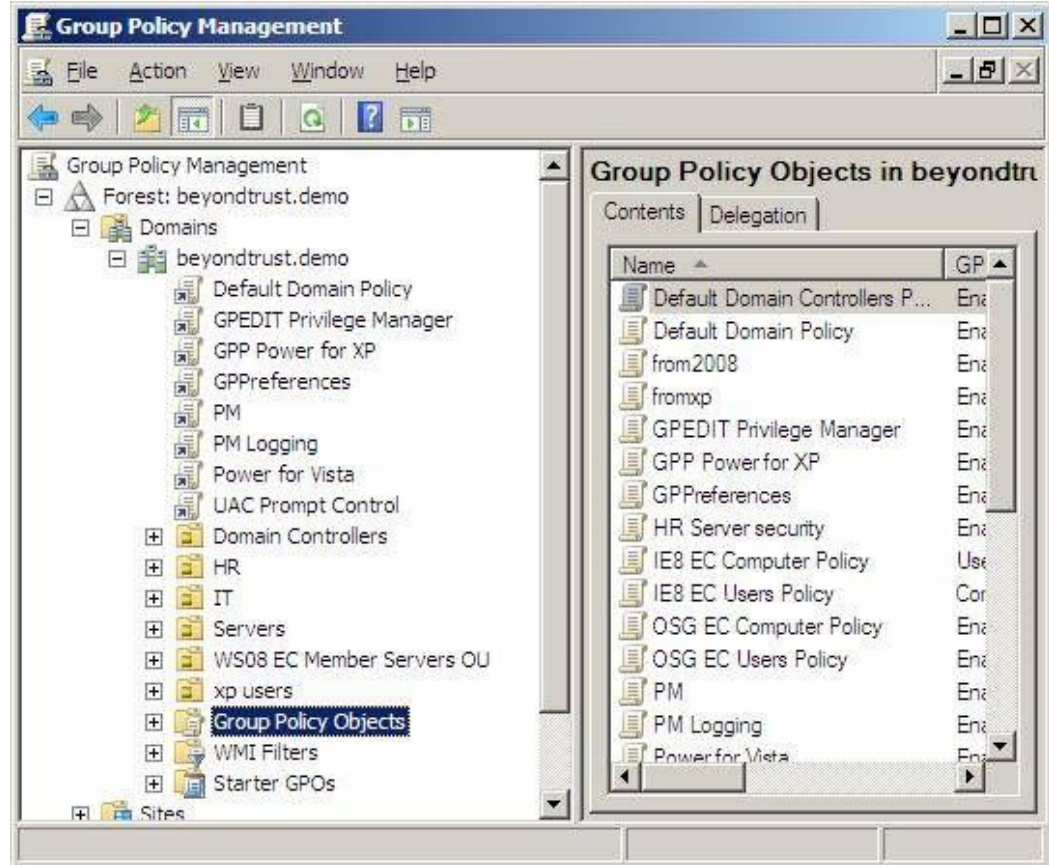
Group Policy

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

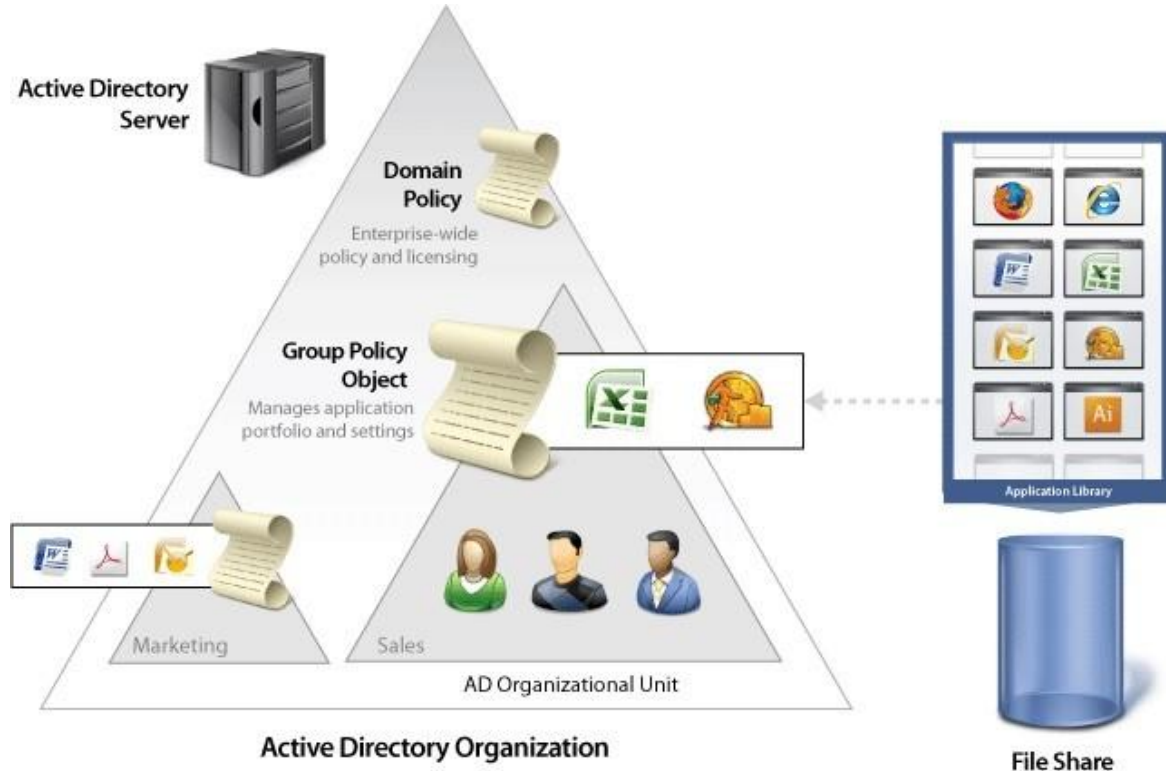
Multiple Group Policies

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



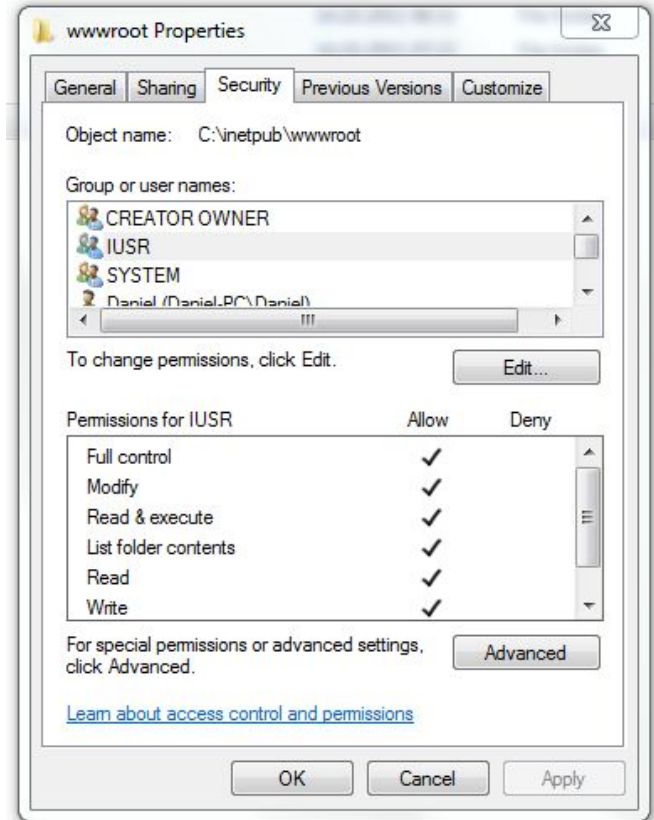
Active directory and Group Policy

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

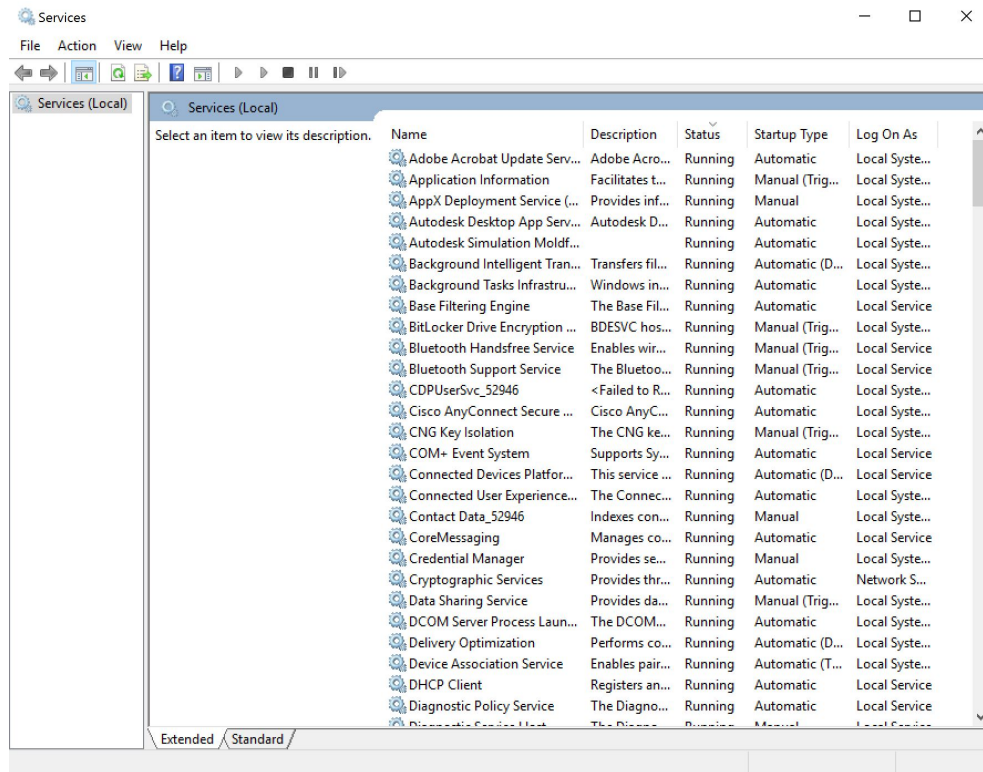


File Permissions

- 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

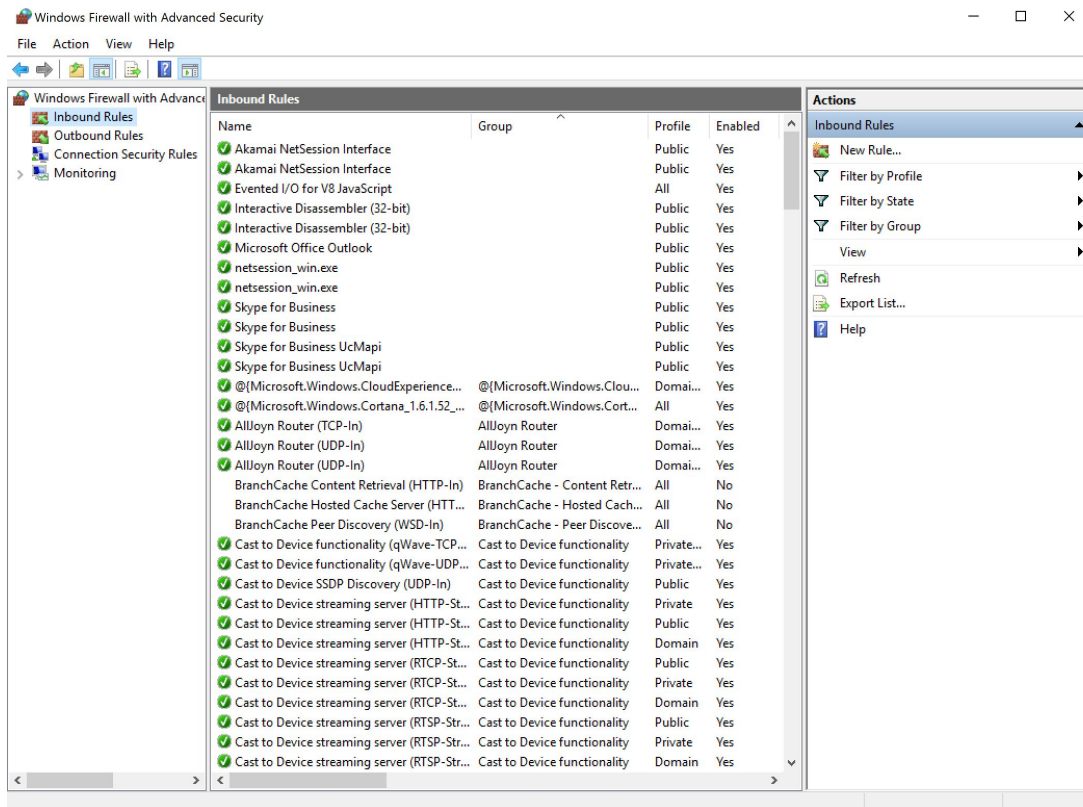


Windows Services (not roles and features)



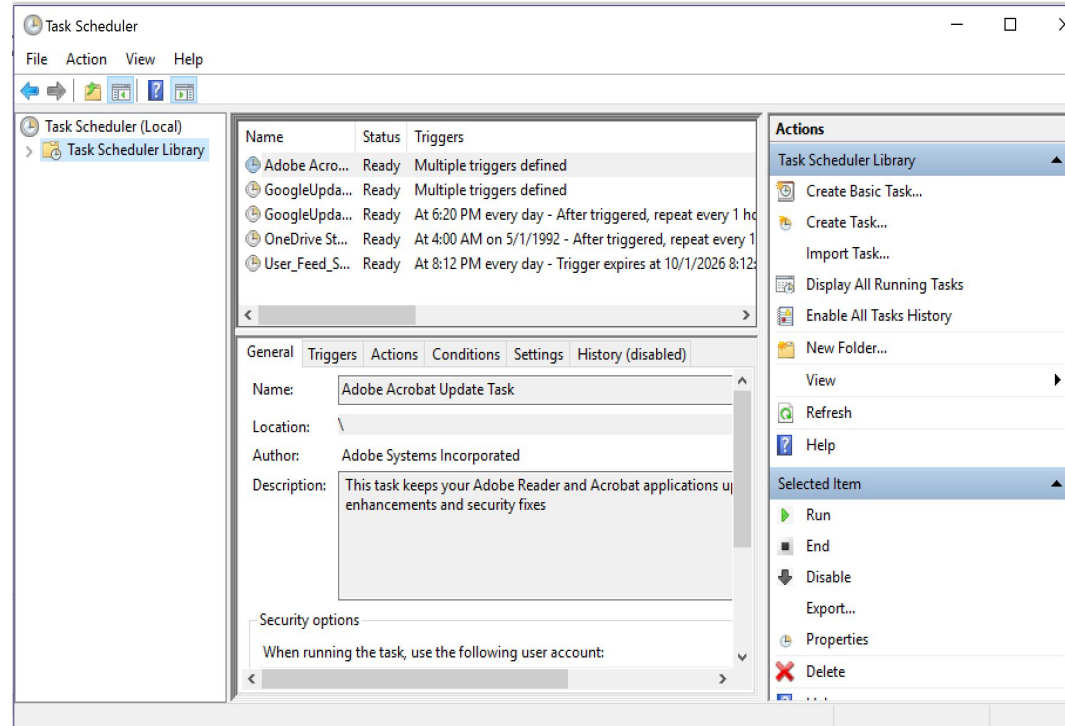
Windows Firewalls

- 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



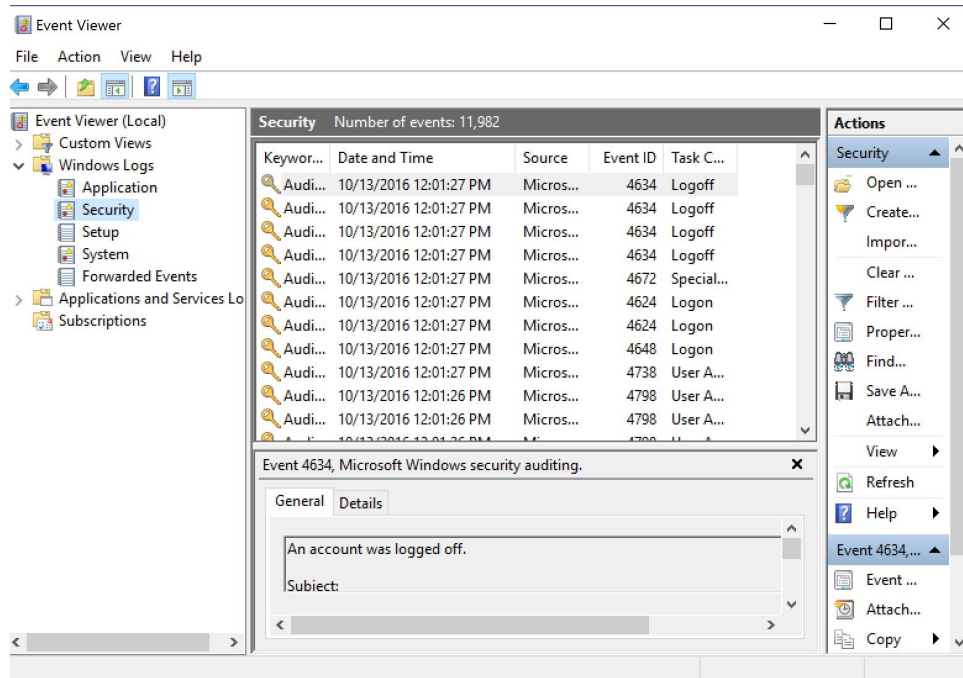
Task Scheduler

- 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

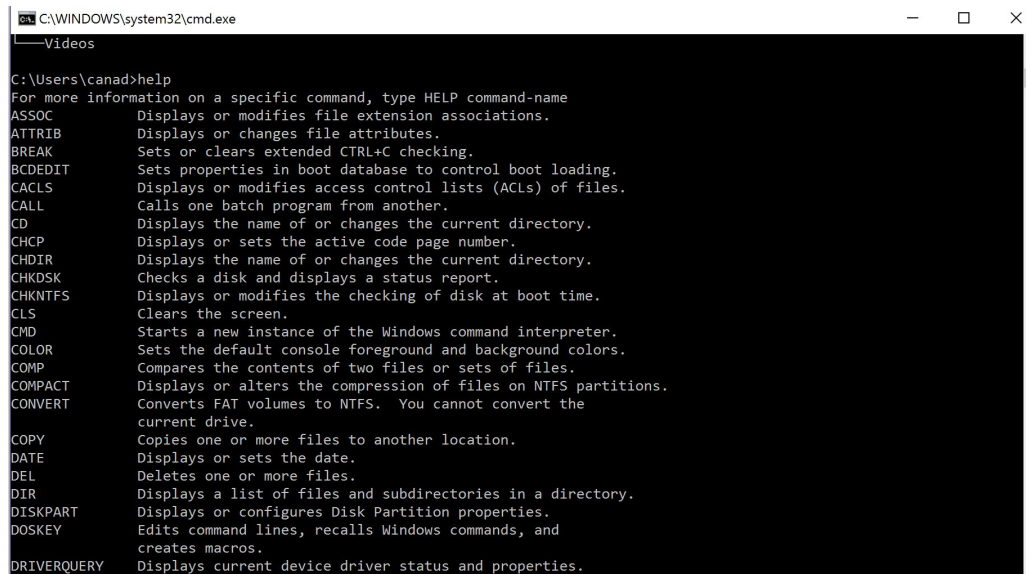
- Monitors all system and application events
- Can be overwhelming
- Useful for troubleshooting
- Useful for looking for bad guys
- Centralized logging
 - Can send all logs to one server, aggregate data for analysis



Command line

- Basic windows commands

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



```
CA\WINDOWS\system32\cmd.exe
Videos
C:\Users\canad>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.
DRIVERQUERY Displays current device driver status and properties.
```

Powershell

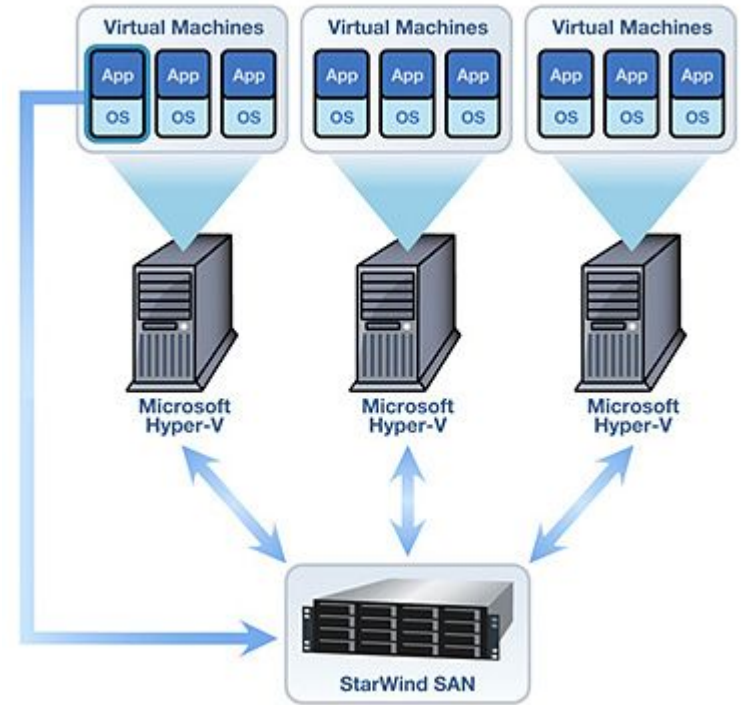
- Can do anything using powershell that you can do using GUI
- Just need to find the right commands
- Can create user and add them to group

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

- Google is your friend

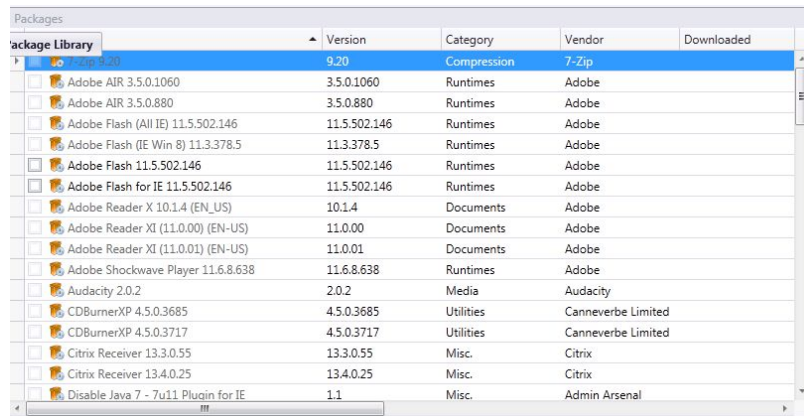
Virtualization

- 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



The screenshot shows the 'Packages' window in Windows Admin Tools. It displays a table of software packages with columns for Name, Version, Category, Vendor, and Downloaded. The 'Package Library' tab is selected, showing a list of various applications including Adobe AIR, Adobe Flash, Adobe Reader, Audacity, CDBurnerXP, and Citrix Receiver.

Package Name	Version	Category	Vendor	Downloaded
Package Library				
7-Zip 6.0.0	9.20	Compression	7-Zip	
Adobe AIR 3.5.0.1060	3.5.0.1060	Runtimes	Adobe	
Adobe AIR 3.5.0.880	3.5.0.880	Runtimes	Adobe	
Adobe Flash (All IE) 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Flash (IE Win 8) 11.3.378.5	11.3.378.5	Runtimes	Adobe	
Adobe Flash 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Flash for IE 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Reader X 10.1.4 (EN_US)	10.1.4	Documents	Adobe	
Adobe Reader XI (11.0.00) (EN-US)	11.0.00	Documents	Adobe	
Adobe Reader XI (11.0.01) (EN-US)	11.0.01	Documents	Adobe	
Adobe Shockwave Player 11.6.8.638	11.6.8.638	Runtimes	Adobe	
Audacity 2.0.2	2.0.2	Media	Audacity	
CDBurnerXP 4.5.0.3685	4.5.0.3685	Utilities	Canneverbe Limited	
CDBurnerXP 4.5.0.3717	4.5.0.3717	Utilities	Canneverbe Limited	
Citrix Receiver 13.3.0.55	13.3.0.55	Misc.	Citrix	
Citrix Receiver 13.4.0.25	13.4.0.25	Misc.	Citrix	
Disable Java 7 - 7u11 Plugin for IE	1.1	Misc.	Admin Arsenal	

Google