



**Microsoft**

UBNetDef, Fall 2023

Week 4

Austin and Lauren!

# Learning Goals

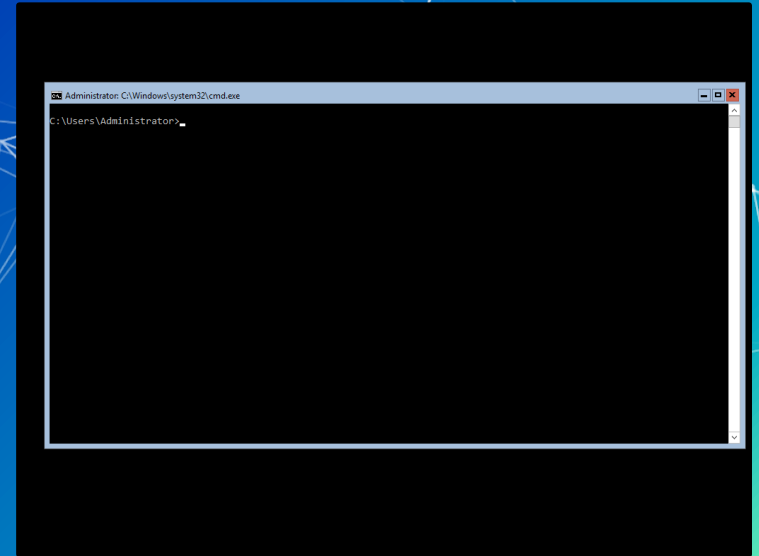
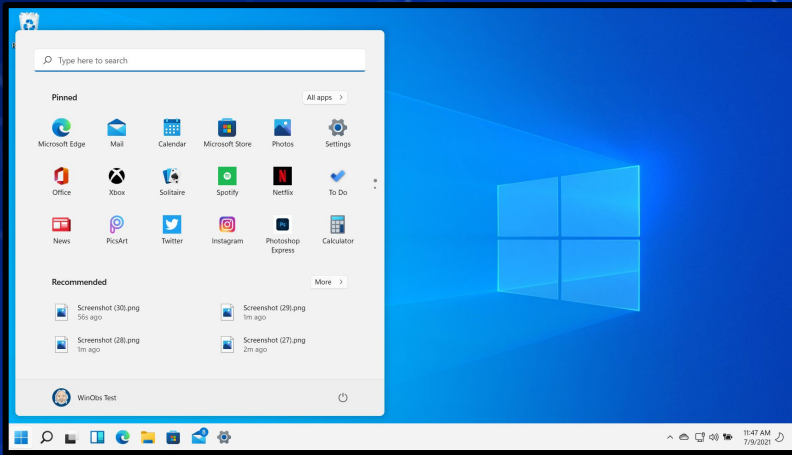
- Understand the difference between Server Desktop and Server Core
- Identify the elements of an Active Directory system
- Create and configure group policy objects
- Distinguish between security groups and organizational units

# 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

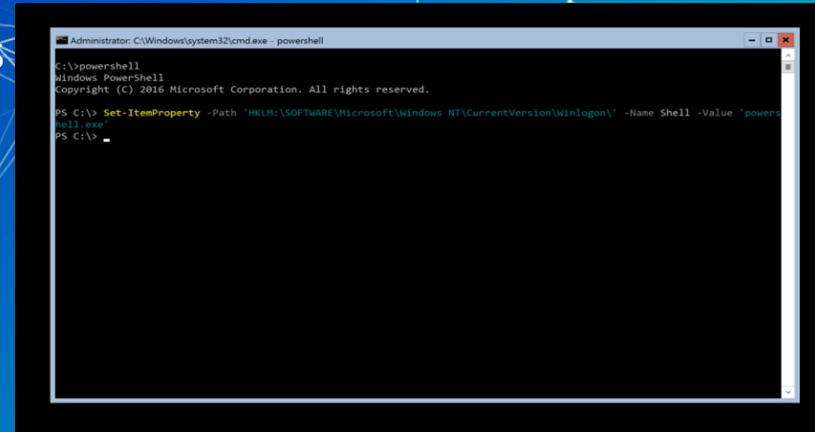
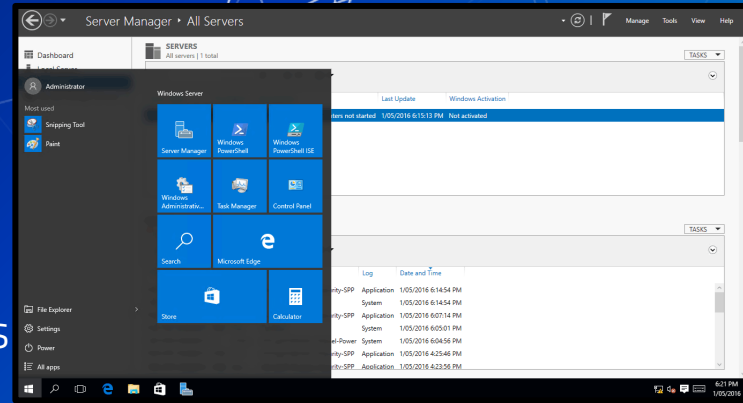
# Windows Server vs. Client

- 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



# 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



# Privileged Accounts

- System is a special type of account
  - Pre-existing
- Administrator account
- **System has the highest privileges on the system**
  - User < Administrator < System

Windows

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

Linux

#root

just **sudo** it





# 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  - Outdated, usually avoid using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. Active Directory
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW



# In Class Activity

Installing Windows Server

orlystei  
pcfox  
pngebura  
radhikaj  
sdileto  
seanmanl  
shreyala  
sames5  
vasudevb  
CompTestEr  
Templates  
ADServerEx  
kaliCPTC  
VasuKali  
WikiJS  
KaliinClass  
LSHHW  
WindowsInC  
SysSec  
Templates  
Lockdown Tem  
SysSec Templa  
Lockdown-v10

Recent Tasks Alarms

Task Name


Status

Actions - ADServerExample

- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...

Guest OS: M  
Compatibility: E  
VMware Tools: N  
DNS Name:  
IP Addresses:  
Host: C

not installed on this virtu



### Edit Settings | ADServerExample

Virtual Hardware | VM Options

ADD NEW DEVICE

CPU	4		
Memory	8	GB	
Hard disk 1	40	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	generic-net		<input checked="" type="checkbox"/> Connected
CD/DVD drive 1	Datastore ISO File		<input type="checkbox"/> Connected
USB controller	USB 2.0		
Video card	Auto-detect settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
SATA controller 0	AHCI		
Other	Additional Hardware		

CANCEL OK

Datstores	Contents
> FTP	en_windows_xp_professional_NO_PROD.
> Homework Engine	vm SCSI-1.2.0.4.flp
> HPEBIOS	w2k3sp2_3959_usa_x64fre_spcd.iso
> IIS	Win10_2004_English_x64.iso
> Internal DB	WIN2019DataCenter.iso
> Internal DNS	Windows 2003 Server.iso
> IPA	Windows10_CLIENT_LTSC_EVAL_x64FRE
✓ ISOs	us.iso
> BSD	Windows_2008_Server.iso
> Linux	Windows_2021_09_19.iso
> LockdownHS	WindowsServer2019Eval.iso
> macOS	WindowsServer2022Eval.iso
> Routers	WinXPSCSI.flp
> Uploaded Templates	

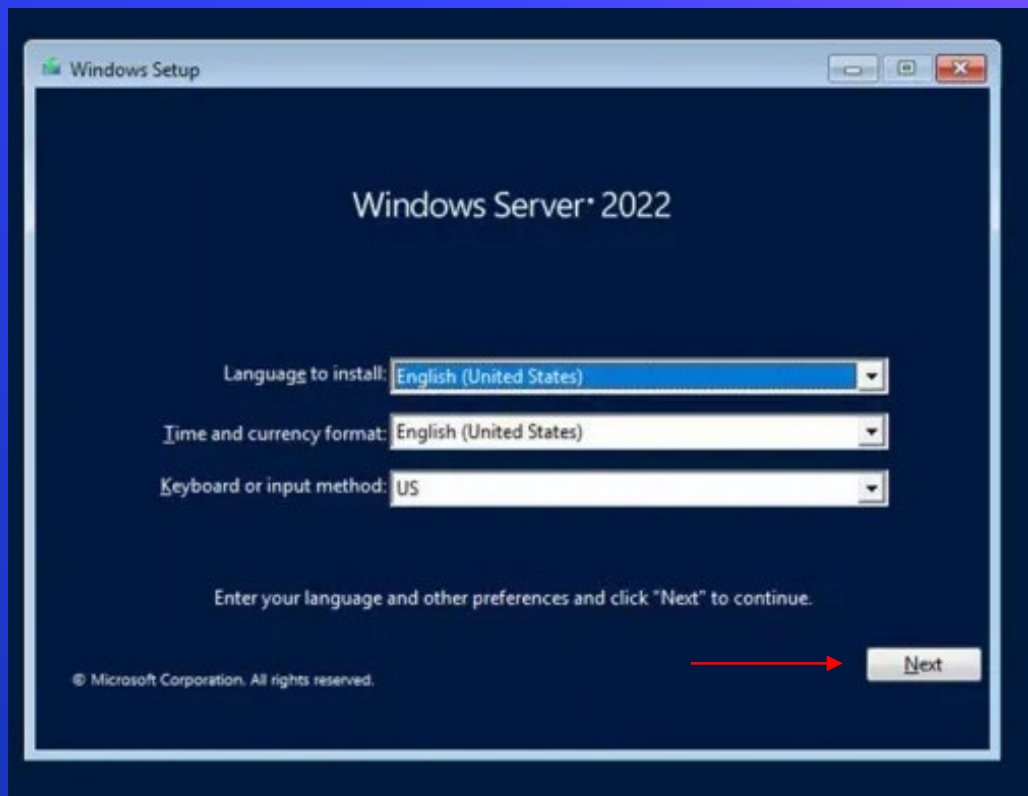
Edit Settings | ADServerExample

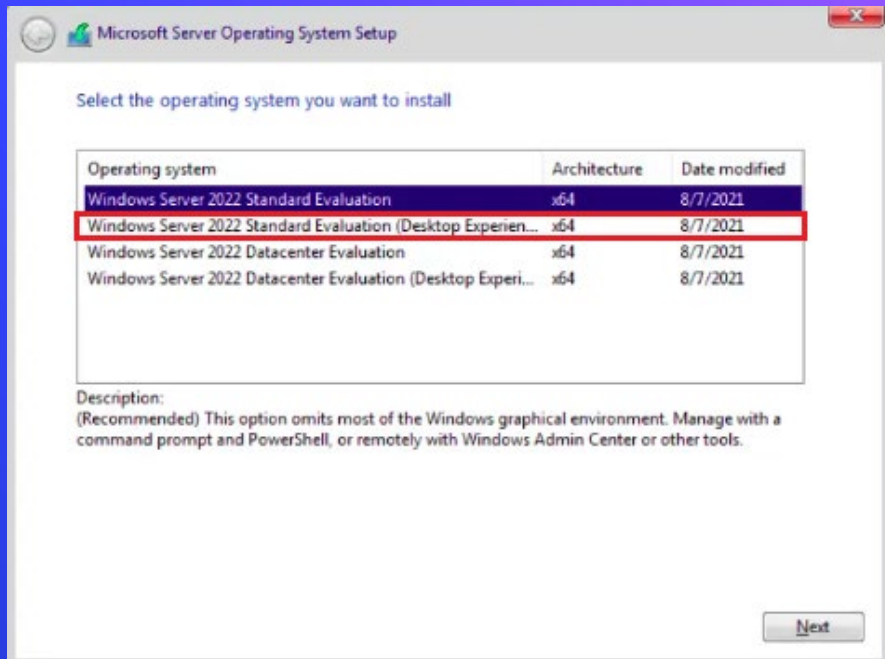
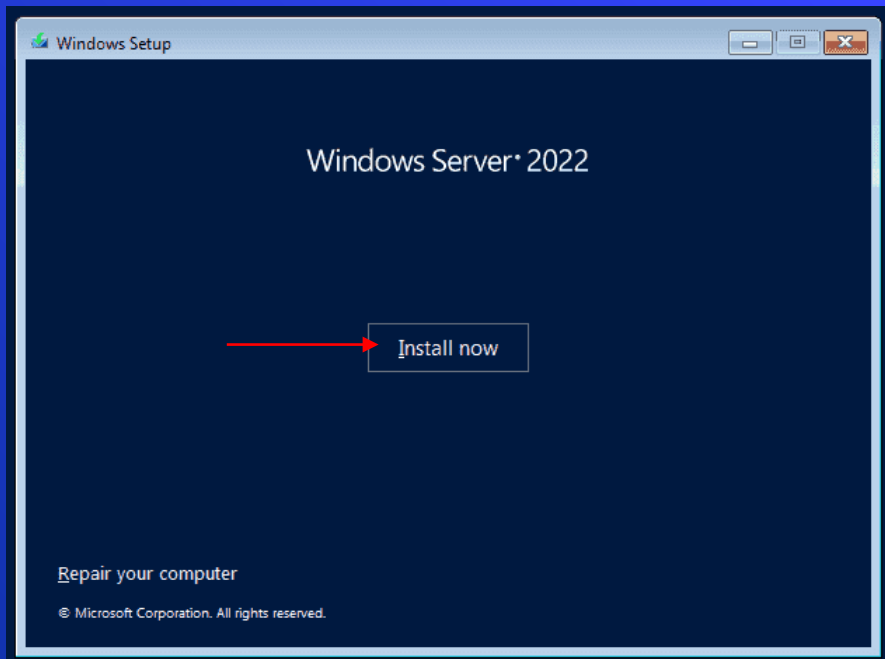
Virtual Hardware | VM Options

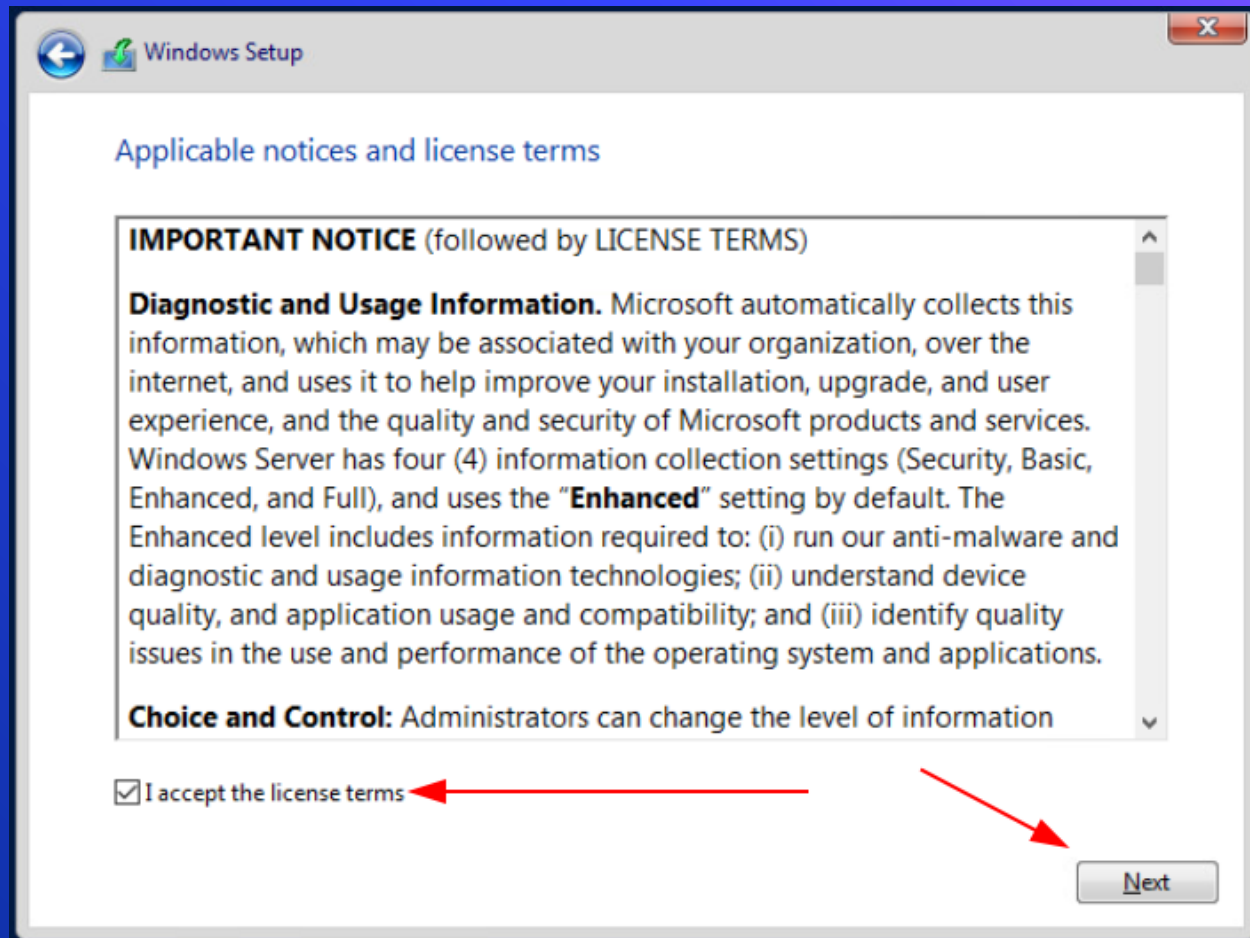
ADD NEW DEVICE

> CPU	4	
> Memory	8	GB
> Hard disk 1	40	GB
> SCSI controller 0	LSI Logic SAS	
> Network adapter 1	generic-net	<input checked="" type="checkbox"/> Connected
> CD/DVD drive 1 *	Datstore ISO File	<input checked="" type="checkbox"/> Connected
Status	<input checked="" type="checkbox"/> Connect At Power On	
CD/DVD Media	[cdr-iscsi] ISOs/Windows	BROWSE...
Device Mode	Passthrough CD-ROM	
Virtual Device Node	SATA controller 0	SATA(0:0) CD/DVD drive 1
> USB controller	USB 2.0	
> Video card	Auto-detect settings	
VMCI device	Device on the virtual machine PCI bus that provides support for the	

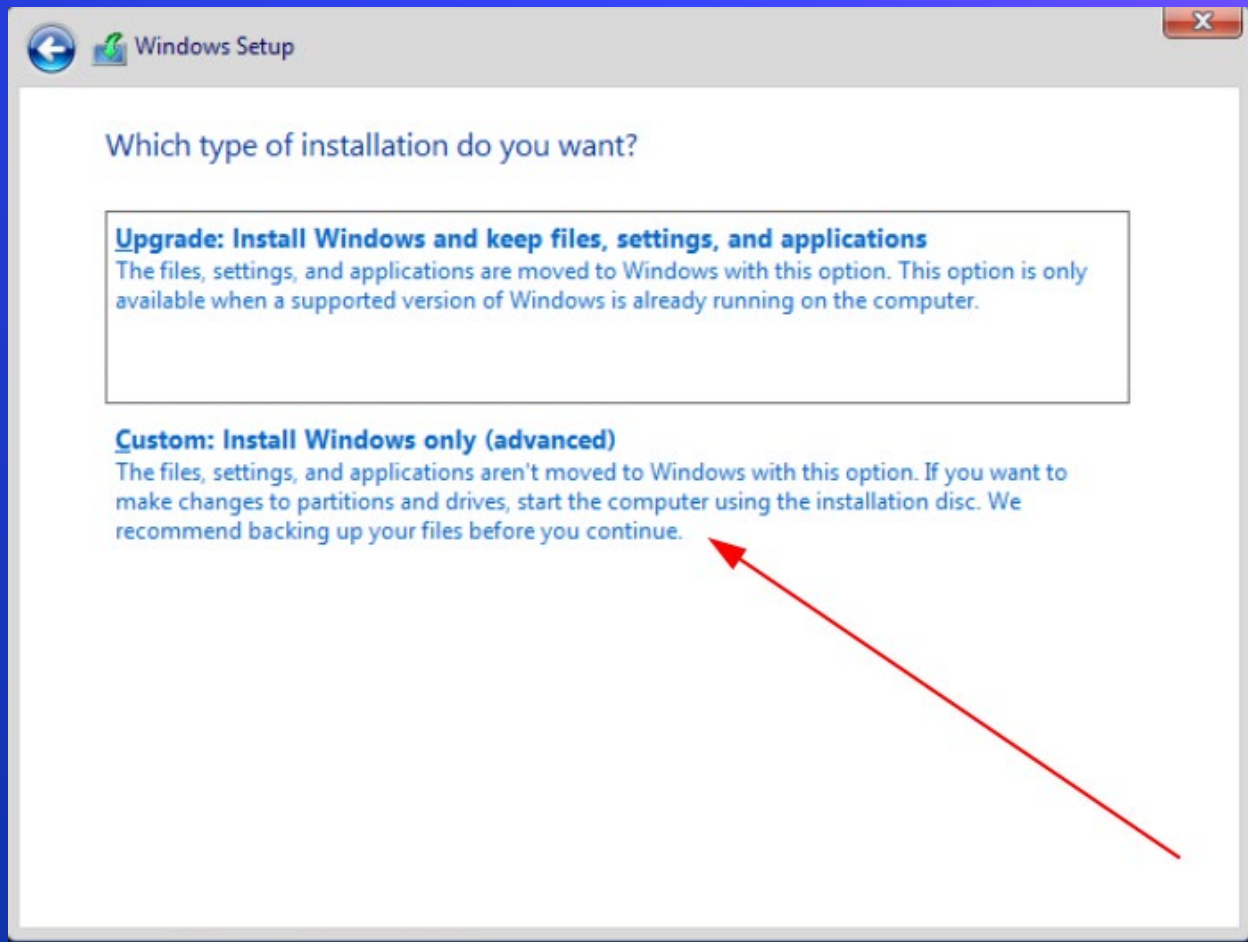
CANCEL OK

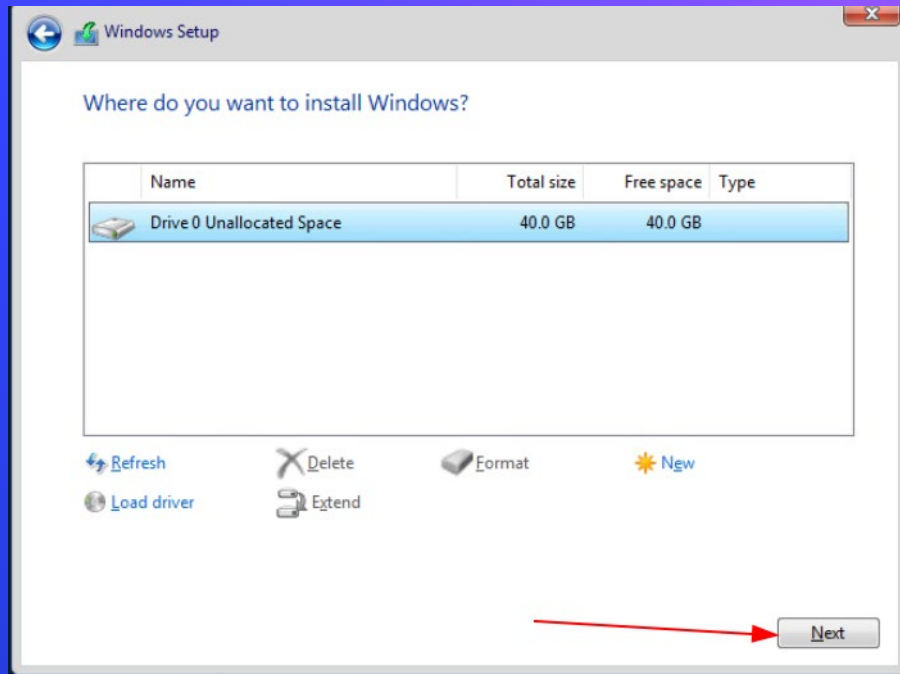
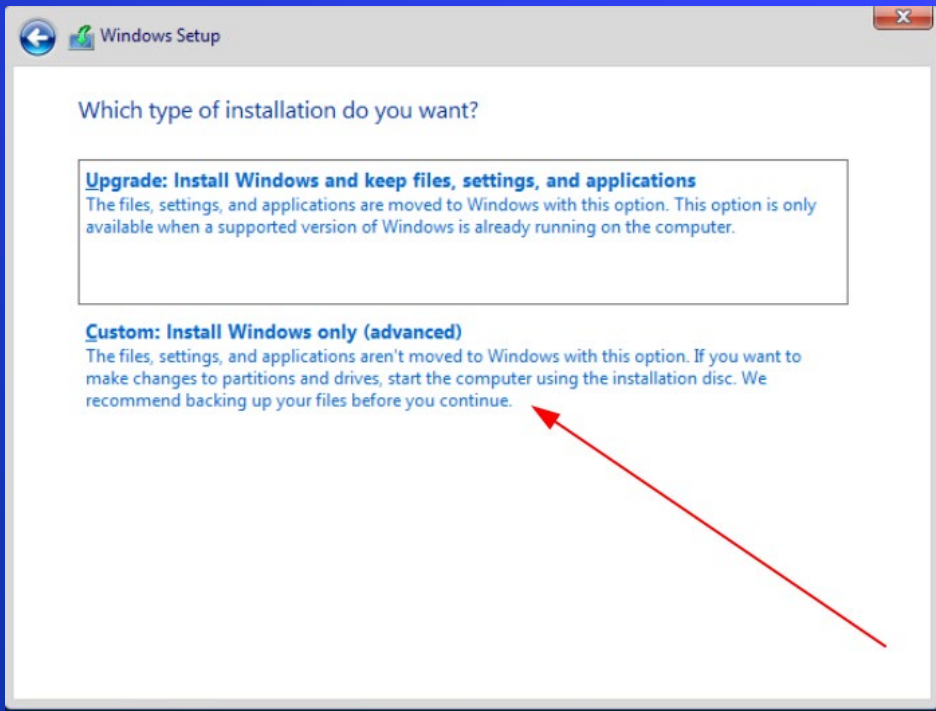












# Agenda

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

# Services and Processes

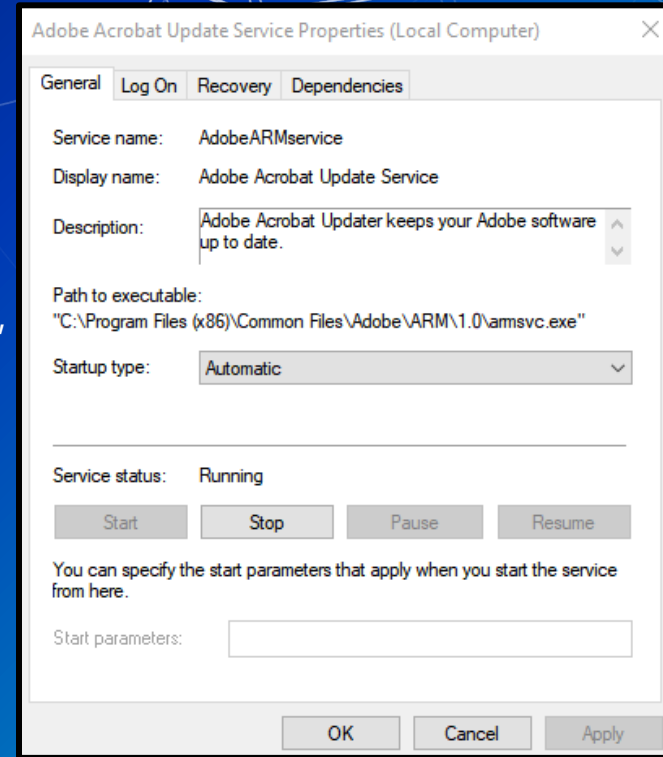
## ■ Services and Processes

- 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 BcastDVRUserSer... Broadcast User 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)
  - Active Directory
    - Identity and Access Management



# 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

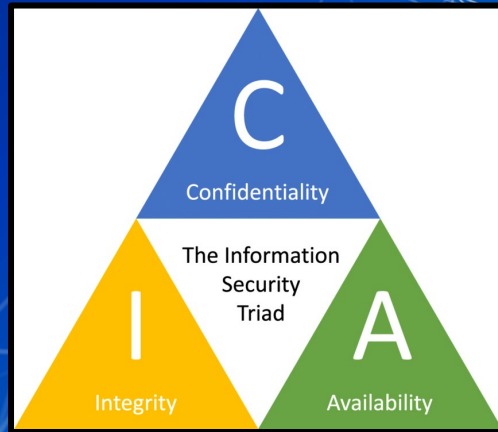
# Identity and Access Management (IAM)

## ■ 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
    - Password
  - Something the user has
    - Duo, Secondary device
  - Something the user is
    - Biometrics (Fingerprint)
    - Less commonly used
- Case in point: vCenter, UBLearns

# QUESTIONS?

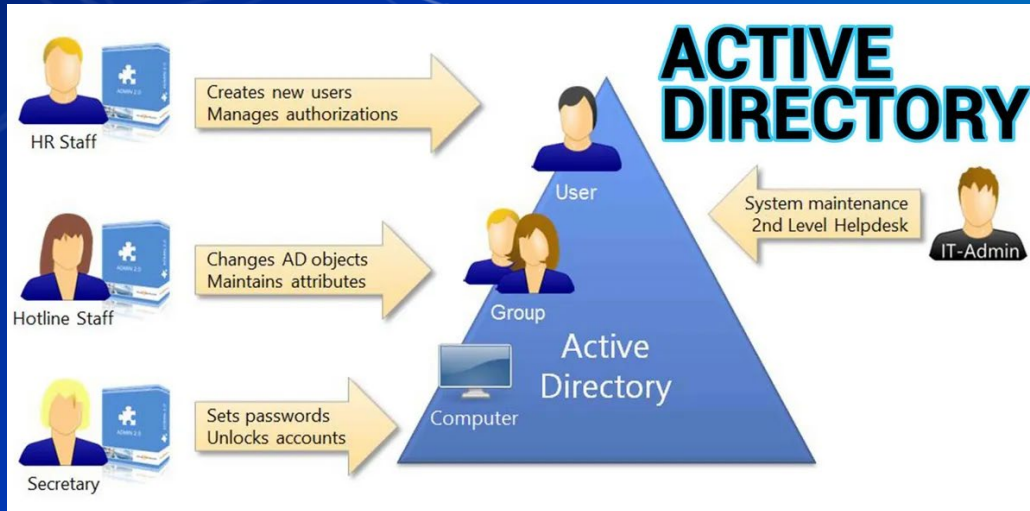
IAM can be complicated, but powerful.

# Agenda

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

# Active Directory

- AD is a directory service for Windows domain networks
  - Controls access to each object based on user authorization
- Objects are users, computers, files, anything networked



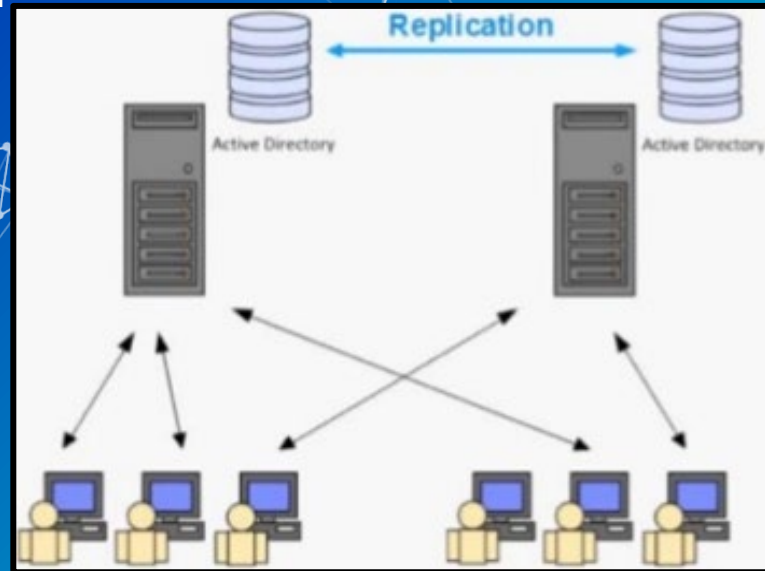


# Components of Active Directory (AD)

- 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)
  - Domain controllers handle IAM
  - The Domain Controller serves Active Directory to Windows domain network.

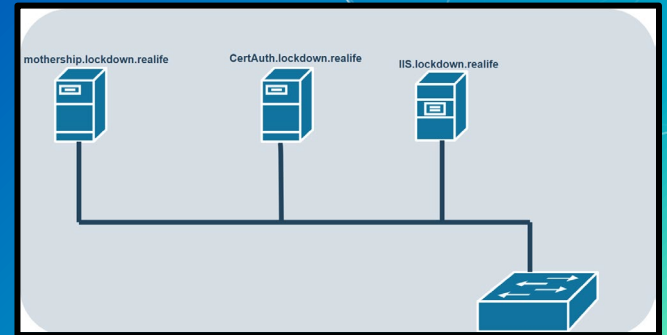
# Domain Controllers (DCs)

- Can have multiple Domain Controllers to have redundancy or server load balancing
- Handles authentication requests for the domain
  - May require running DNS
  - Will require Network Time Protocol (NTP)
  - And more!



# AD and DNS

- AD uses DNS so that clients can locate domain controllers and communicate with each other.
  - IP's can change.
  - AD computer names are unique per domain.
- Domain controllers (that run AD) also can serve as the local AD DNS & DHCP server.
  - DHCP automatically assigns IPs.



# Agenda

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

# In Class Activity

Setting up static IP and DNS

ADServerInClass

Enforce US Keyboard Layout

View Fullscreen

Send Ctrl+Alt+Delete



netdef

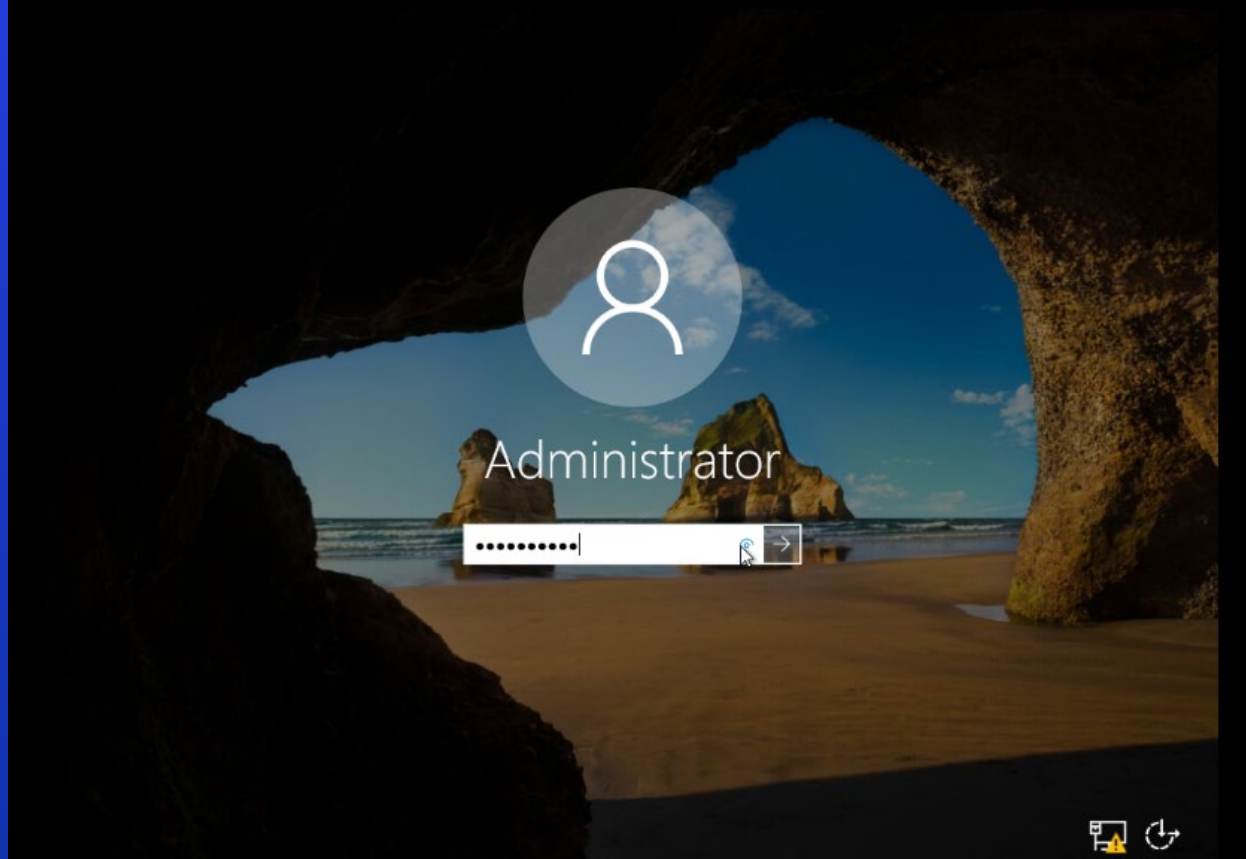
Press Ctrl+Alt+Delete to unlock.

5:22

Thursday, September 23

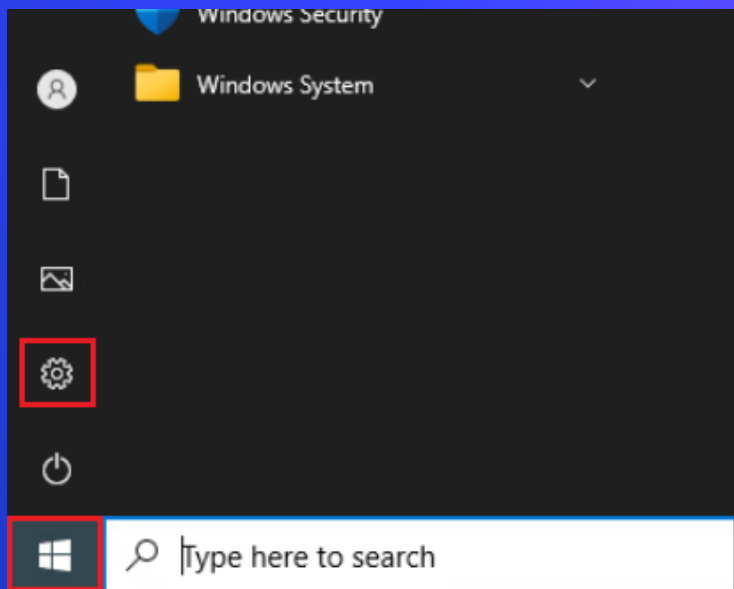








NetDef





## Windows Settings

Find a setting



### System

Display, sound, notifications,  
power



### Devices

Bluetooth, printers, mouse



### Network & Internet

Wi-Fi, airplane mode, VPN



### Personalization

Background, lock screen, colors



### Apps

Uninstall, defaults, optional  
features



### Accounts

Your accounts, email, sync,  
work, other people



### Time & Language

Speech, region, date



### Ease of Access

Narrator, magnifier, high  
contrast



Home


Find a setting

Network & Internet

- Status
- Ethernet
- Dial-up
- VPN
- Proxy

## Status

### Network status



Unidentified network  
Public network

**You're connected to the Internet**

You're on a metered network. Some apps might work differently to help you save data while on this network.

Troubleshoot


Show available networks  
View the connection options around you.


### Advanced network settings

- Change adapter options  
View network adapters and change connection settings.




NetDef

 Network Connections

← → ▾ ↑  << Network and Internet >> Network Connections >

Organize ▾

 **Ethernet0**  
Unidentified network  
Intel(R) 82574L Gigabit Network C...



# NetDef

Ethernet0 Status


General

Connection

IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	17:24:33
Speed:	1.0 Gbps

Details...

Activity

Sent —  — Received

Bytes: 0 | 120

Properties Disable Diagnose

Close



# NetDef

Ethernet0 Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- QoS Packet Scheduler
- Internet Protocol Version 4 (TCP/IPv4)
- Microsoft Network Adapter Multiplexor Protocol
- Microsoft LLDP Protocol Driver
- Internet Protocol Version 6 (TCP/IPv6)

Install... Uninstall Properties

Description

Allows your computer to access resources on a Microsoft network.

OK Cancel

001

011

010





Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

**Use your team number**

Obtain an IP address automatically

Use the following IP address:

IP address: 10 . 42 . 30 . 98

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 42 . 30 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

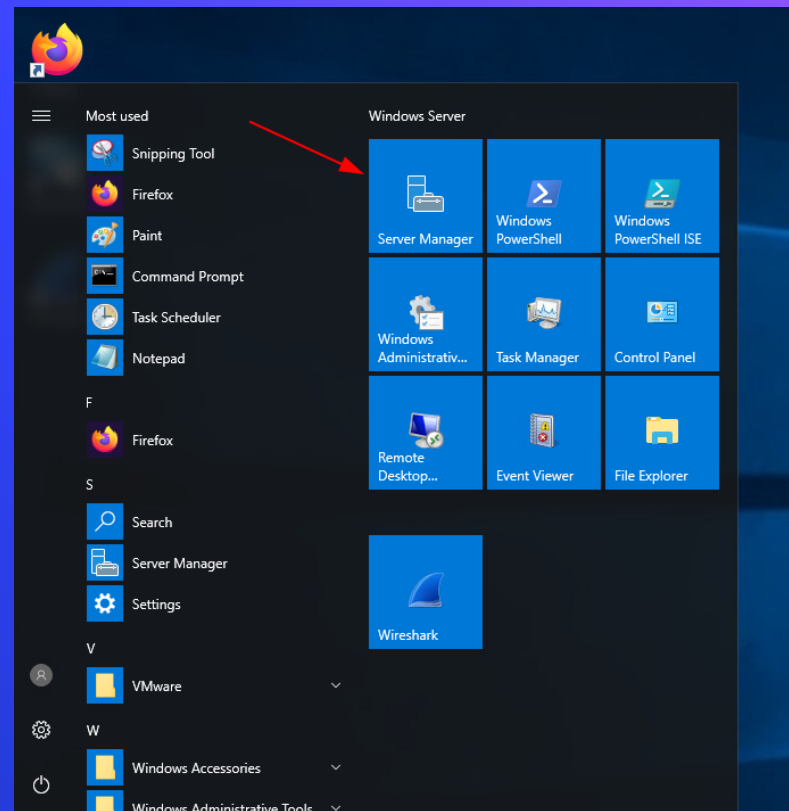
Preferred DNS server: 127 . 0 . 0 . 1

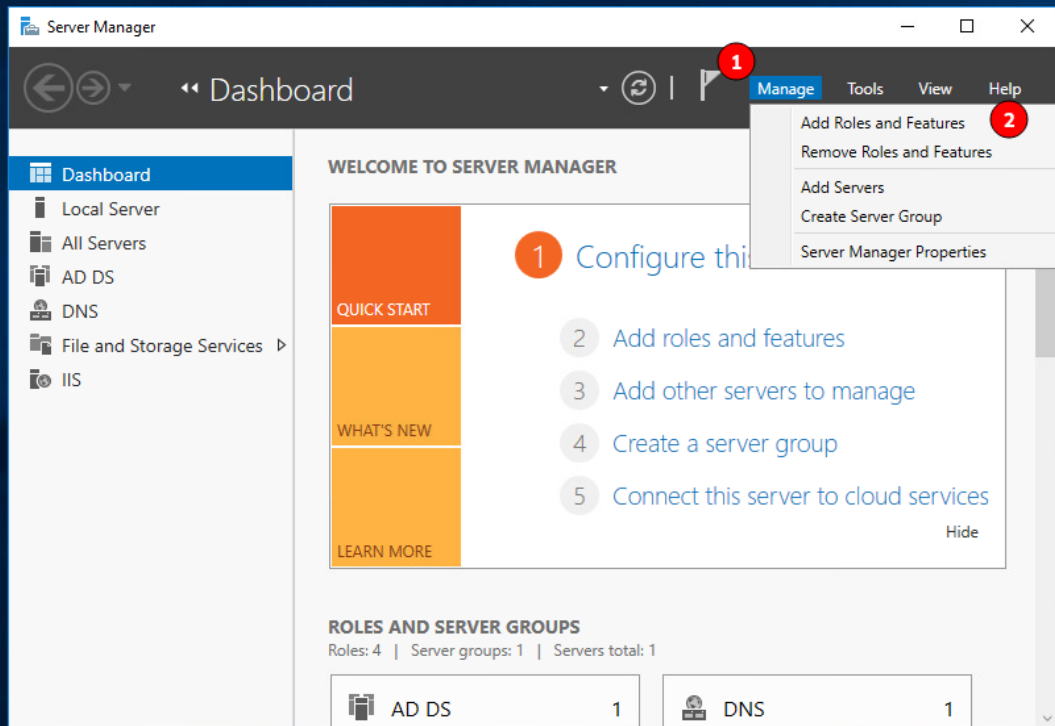
Alternate DNS server: . . .

Validate settings upon exit

Advanced...

OK Cancel





The screenshot shows the Windows Server Manager interface. The 'Manage' menu is open, and a '1' is placed over the menu icon. A '2' is placed over the 'Add Roles and Features' option in the menu. A '1' is placed over the first step in the 'QUICK START' list. A '2' is placed over the second step in the list.

Server Manager

Dashboard

Local Server

All Servers

AD DS

DNS

File and Storage Services

IIS

WELCOME TO SERVER MANAGER

1 Configure this server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

Hide

ROLES AND SERVER GROUPS

Roles: 4 | Server groups: 1 | Servers total: 1

AD DS	1	DNS	1
-------	---	-----	---

Add Roles and Features Wizard

Before you begin

DESTINATION SERVER  
Concord.mothership.local

**Before You Begin**

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:  
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:


- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous   **Next >**   Install   Cancel



## Select installation type

DESTINATION SERVER  
Concord.mothership.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

&lt; Previous

Next &gt;

Install

Cancel



## Select destination server

DESTINATION SERVER  
WIN-KMSA6VBDJA4

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool  
 Select a virtual hard disk

## Server Pool

Filter: 

Name	IP Address	Operating System
WIN-KMSA6VBDJA4	169.254.197.115	Microsoft Windows Server 2019 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

&lt; Previous

Next &gt;

Install

Cancel





Add Roles and Features Wizard

DESTINATION SERVER  
WIN-KMSA6VBDJA4

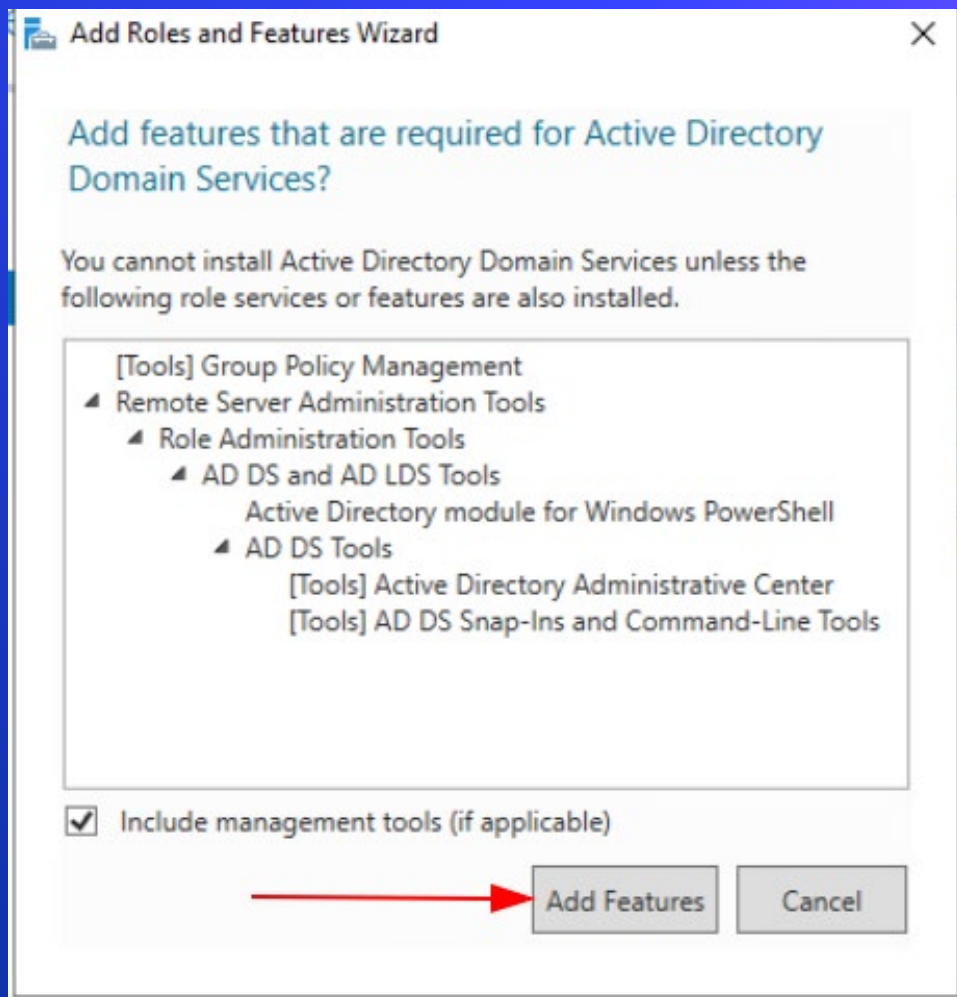
## Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Select one or more roles to install on the selected server.

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	
<input type="checkbox"/> <b>Active Directory Domain Services</b>	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Update Services	

< Previous   Next >   Install   Cancel





### Select server roles

DESTINATION SERVER  
WIN-KMSA6VBDJA4

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

AD DS

Confirmation

Results

Select one or more roles to install on the selected server.

#### Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- ▶  File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

#### Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

Next >

Install

Cancel



Add Roles and Features Wizard

### Add features that are required for DNS Server?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

Include management tools (if applicable)



**Add Roles and Features Wizard**

DESTINATION SERVER  
WIN-KMSA6VBDJA4

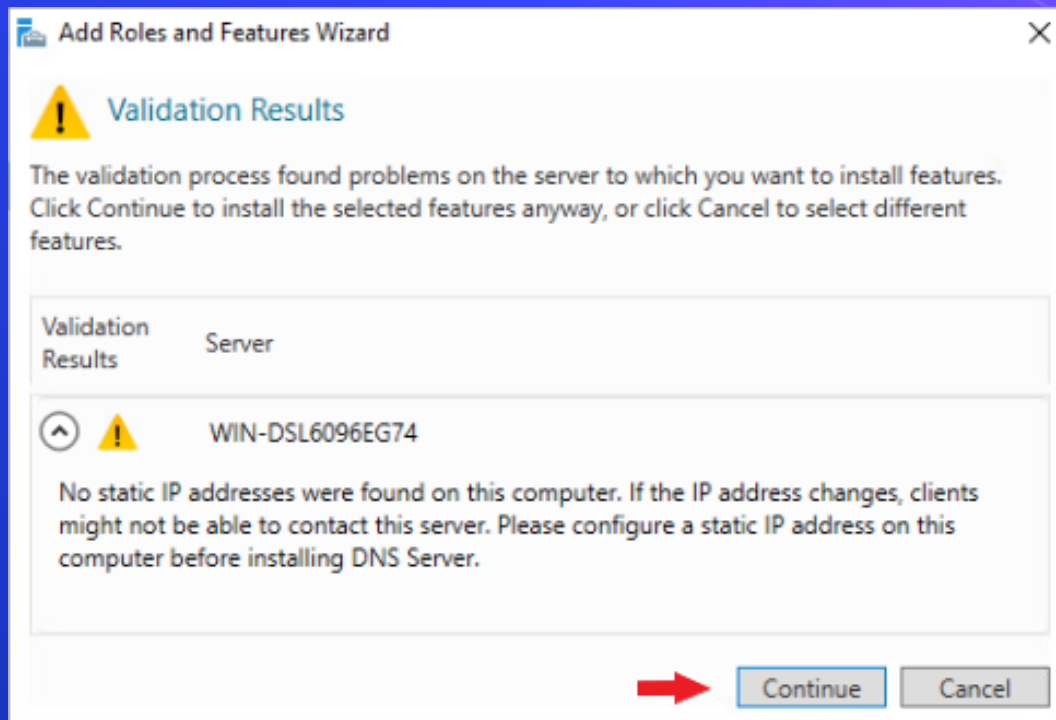
## Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
AD DS  
DNS Server  
Confirmation  
Results

Select one or more roles to install on the selected server.

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
<input checked="" type="checkbox"/> Active Directory Domain Services	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input checked="" type="checkbox"/> <b>DNS Server</b>	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Update Services	

< Previous   **Next >**   Install   Cancel



You might get this warning message



Add Roles and Features Wizard

DESTINATION SERVER  
WIN-T1A54RB8L8M

## Select features

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
**Features**  
AD DS  
DNS Server  
Confirmation  
Results

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management	Group Policy Management is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. Group Policy Management is the standard tool for managing Group Policy.
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> LPR Port Monitor	

< Previous   Next >   Install   Cancel



DESTINATION SERVER  
WIN-KMSA6VBDJA4

## Active Directory Domain Services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

**AD DS**

DNS Server

Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

## DNS Server

DESTINATION SERVER  
WIN-KMSA6VBDJA4

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD DS  
**DNS Server**  
Confirmation  
Results

Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.

< Previous   Next >   Install   Cancel



### Confirm installation selections

DESTINATION SERVER  
WIN-KMSA6VBDJA4

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

**Confirmation**

Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- DNS Server
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - DNS Server Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
    - AD DS Tools
      - Active Directory Administrative Center
      - AD DS Snap-Ins and Command-Line Tools

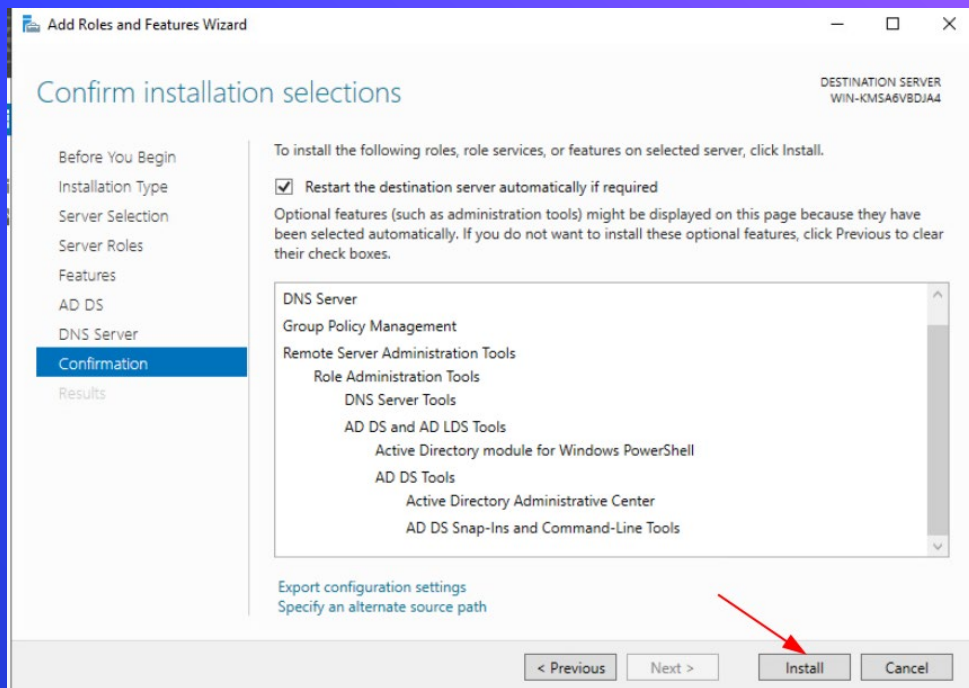
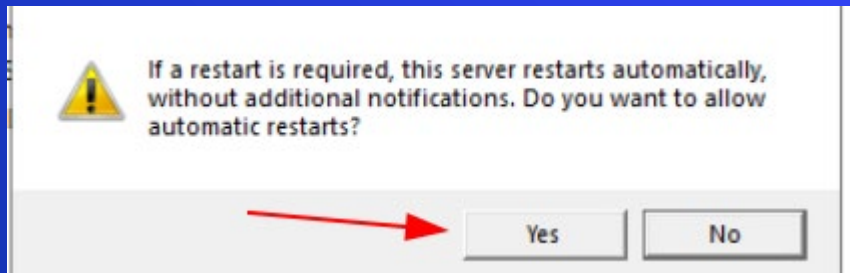
[Export configuration settings](#)  
[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel





### Installation progress

DESTINATION SERVER  
WIN-KMSA6VBDJA4

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

Confirmation

Results

View installation progress

#### Feature installation

Configuration required. Installation succeeded on WIN-KMSA6VBDJA4.

##### Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

##### DNS Server

##### Group Policy Management

##### Remote Server Administration Tools

##### Role Administration Tools

##### DNS Server Tools

##### AD DS and AD LDS Tools

##### Active Directory module for Windows PowerShell

##### AD DS Tools



You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

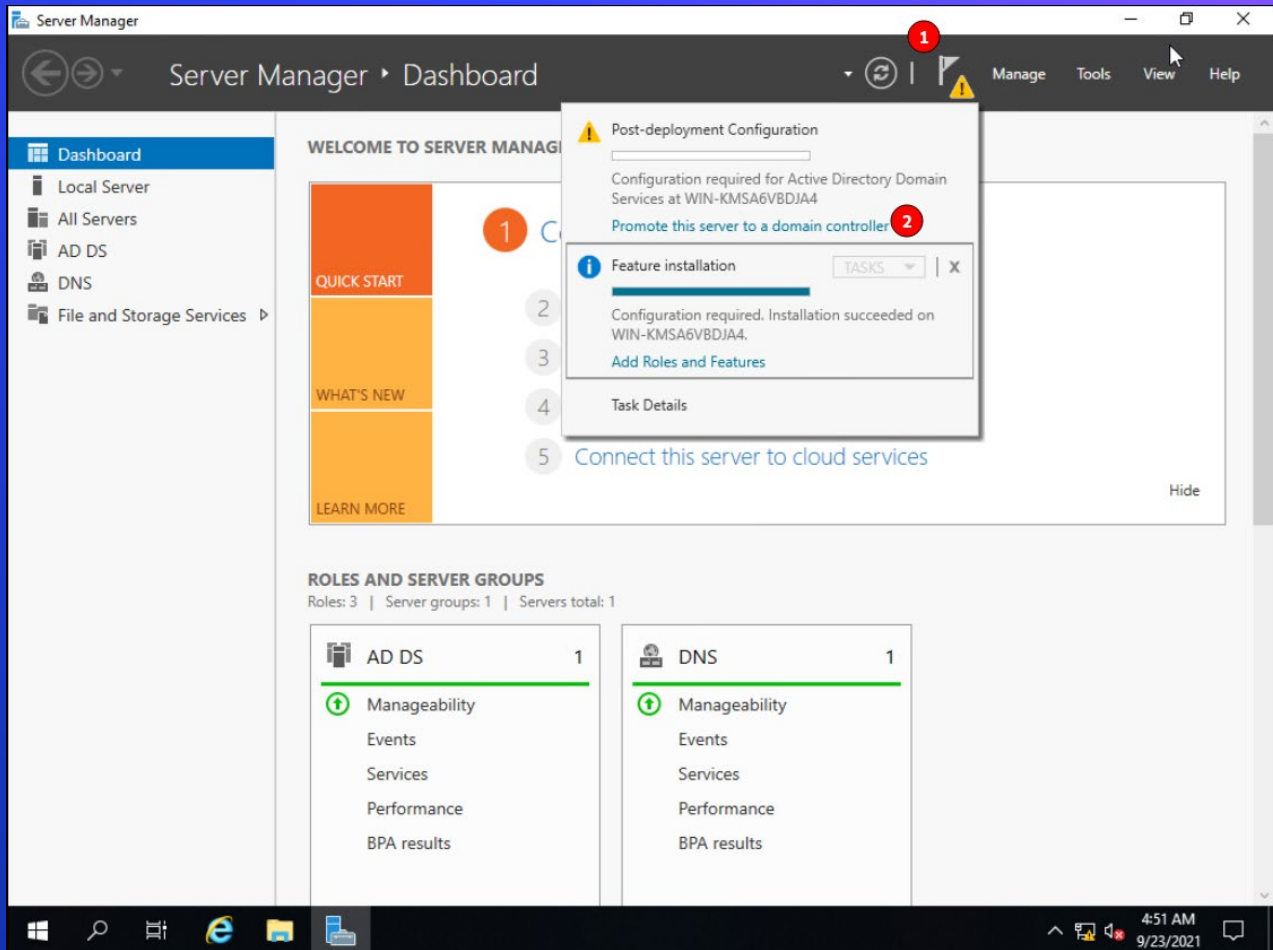
< Previous

Next >

Close

Cancel





The screenshot shows the Windows Server Manager interface. The top navigation bar includes 'Server Manager' and 'Dashboard'. A left-hand navigation pane lists 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main content area is titled 'WELCOME TO SERVER MANAGER' and contains a 'QUICK START' section with buttons for 'WHAT'S NEW' and 'LEARN MORE'. A vertical list of numbered steps (1-5) is visible: 1. Connect this server to cloud services, 2. Add Roles and Features, 3. Configure the server, 4. Add server to a server group, 5. Connect this server to cloud services. A 'Post-deployment Configuration' notification is open, showing a warning icon and the text: 'Configuration required for Active Directory Domain Services at WIN-KMSA6VBDJA4. Promote this server to a domain controller.' Below this is a 'Feature installation' notification with an information icon, stating: 'Configuration required. Installation succeeded on WIN-KMSA6VBDJA4. Add Roles and Features. Task Details.' The bottom section, 'ROLES AND SERVER GROUPS', shows 'Roles: 3 | Server groups: 1 | Servers total: 1'. It contains two columns: 'AD DS' with 1 role and 'DNS' with 1 role. Each column lists 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. The Windows taskbar at the bottom shows the time as 4:51 AM on 9/23/2021.



Active Directory Domain Services Configuration Wizard

## Deployment Configuration

TARGET SERVER  
WIN-KMSA6VBDJA4

- Deployment Configuration
- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest **1**

Specify the domain information for this operation

Root domain name: **2**

[More about deployment configurations](#) **3**

< Previous   Next >   Install   Cancel

Use your team number

Active Directory Domain Services Configuration Wizard

## Domain Controller Options

TARGET SERVER  
WIN-DSL6096EG74

- Deployment Configuration
- Domain Controller Options**
- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: [masked]

Confirm password: [masked]

Make password: **Change.me!**

[More about domain controller options](#)

< Previous   **Next >**   Install   Cancel



Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER  
WIN-KMSA6VBDJA4

**⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) ✕**

- Deployment Configuration
- Domain Controller Options
- DNS Options**
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Specify DNS delegation options

Create DNS delegation

[More about DNS delegation](#)

< Previous   **Next >**   Install   Cancel



Active Directory Domain Services Configuration Wizard

## Additional Options

TARGET SERVER  
WIN-KMSA6VBDJA4

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options**
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous   **Next >**   Install   Cancel

## Paths

TARGET SERVER  
WIN-KMSA6VBDJA4

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

**Paths**

Review Options

Prerequisites Check

Installation

Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:  ...

Log files folder:  ...

SYSVOL folder:  ...

[More about Active Directory paths](#)

< Previous

Next >

Install

Cancel



NetDef



Active Directory Domain Services Configuration Wizard

TARGET SERVER  
WIN-KMSA6VBDJA4

## Review Options

- Deployment Configuration
- Domain Controller Options
  - DNS Options
- Additional Options
- Paths
- Review Options**
- Prerequisites Check
- Installation
- Results

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "team99.local". This is also the name of the new forest.

The NetBIOS name of the domain: TEAM99

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations [View script](#)

[More about installation options](#)



< Previous   **Next >**   Install   Cancel



Active Directory Domain Services Configuration Wizard

TARGET SERVER  
WIN-KMSA6VBDJA4


## Prerequisites Check


 All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) 

- Deployment Configuration
- Domain Controller Options
  - DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check**
- Installation
- Results


Prerequisites need to be validated before Active Directory Domain Services is installed on this computer


[Rerun prerequisites check](#)

 View results

 Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

 This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

 If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

[< Previous](#) [Next >](#) **Install** [Cancel](#)

# Break

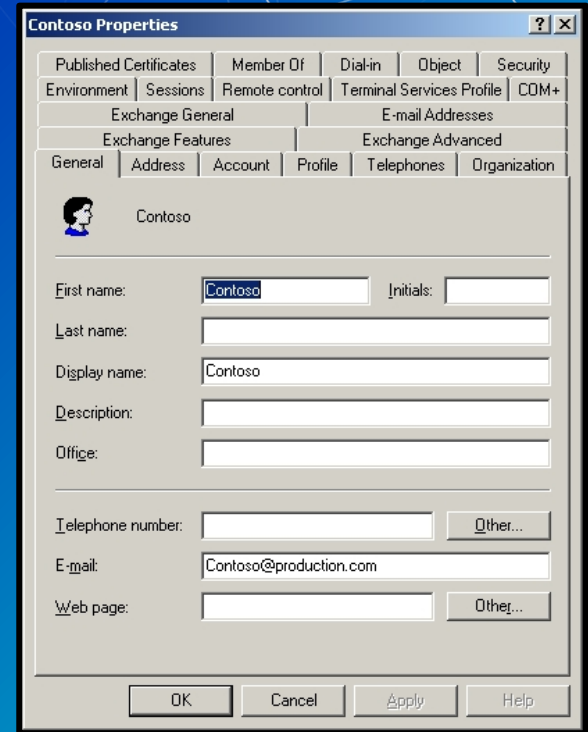
10 mins

# Agenda

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

# Active Directory - User Objects

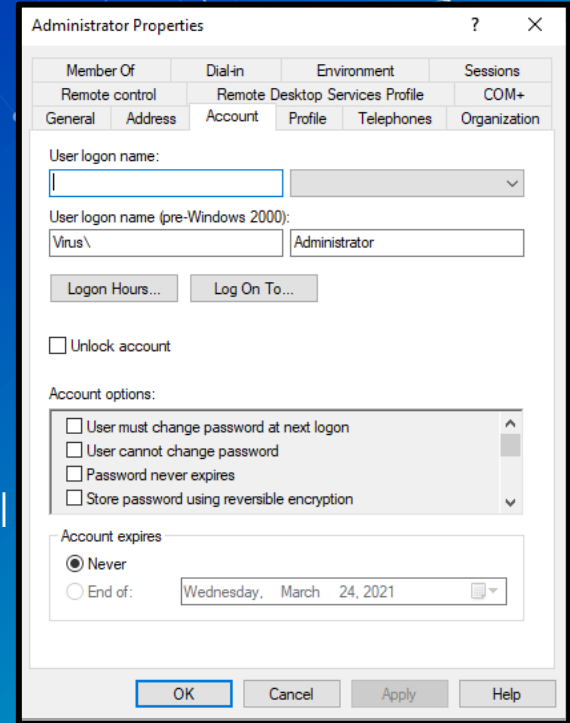
- What people authenticate against when they sign on
- Stores information on user
  - **Username**
  - Display name
  - Email
  - Phone number
  - Address
  - Location in organization
  - **Password (hashed)**



The screenshot shows the 'Contoso Properties' dialog box with the 'General' tab selected. The 'Organization' field is set to 'Contoso'. The 'First name' field contains 'Contoso' and the 'Initials' field is empty. The 'Last name' field is empty. The 'Display name' field contains 'Contoso'. The 'Description' and 'Office' fields are empty. The 'Telephone number' field is empty with an 'Other...' button. The 'E-mail' field contains 'Contoso@production.com'. The 'Web page' field is empty with an 'Other...' button. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

# 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



# Active Directory - Security Concerns

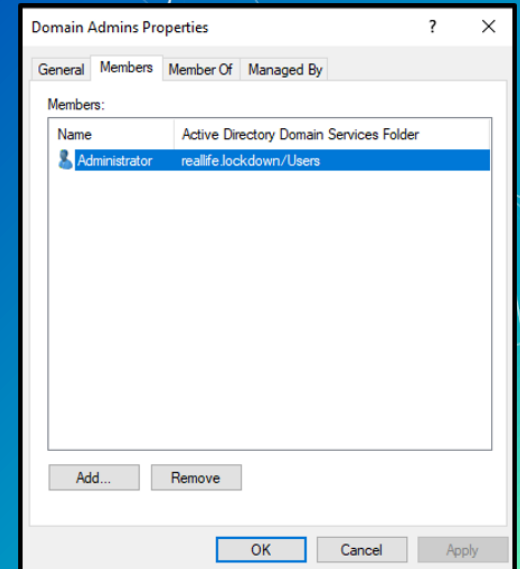
- We need a new object for each user. -> Too many to safely manage
  - UB has about 50,000 users on its main domain
- Security issues:
  - What happens when we need to change permissions on every single student (~30K)
  - What happens when someone leaves?



# Active Directory - 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

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 ...





# North America Division



**Marketing**

**Sales**

**Service**

Name: Jon Pestinger  
Email: [Jon@company.com](mailto:Jon@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? Network Admin? Why?
- Leads to group inheritance



# Active Directory - Inheritance

- Think of trickle down theory
- 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



Parent Group

# North America Division

Child Groups

User Objects

Name: Jon Pestinger  
Email: Jon@company.com  
Department: Marketing  
Phone: 123  
Title: Technical Writer



Marketing

Sales

Service

Only marketing can use Canva!

Only Sales gets Excel!

# 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

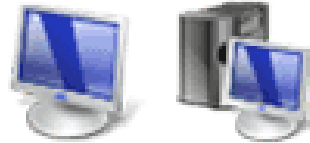
## Supporter

## Computers

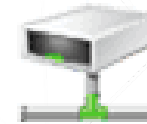
## Applications

### Finance

### Marketing



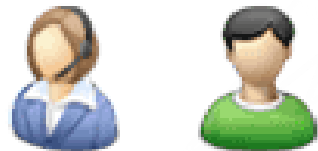
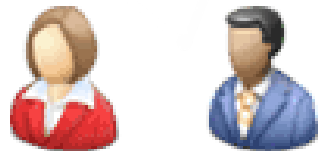
Computers



Network Share



Printers



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

# Active Directory – Organizational Units (OU)

- 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 - Organizational Units (OU)

- Organizational Units (OU) are used to organize Active Directory so it's easier to manage.
- **Differ from Security Groups**
  - Security Groups are going to be IAM based!
    - Access control, membership
  - OUs are for...
    - Administrative control
    - Hierarchy (for organizational control)
    - Group policy management
- **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.

# North America Division

Marketing



Sales



Service



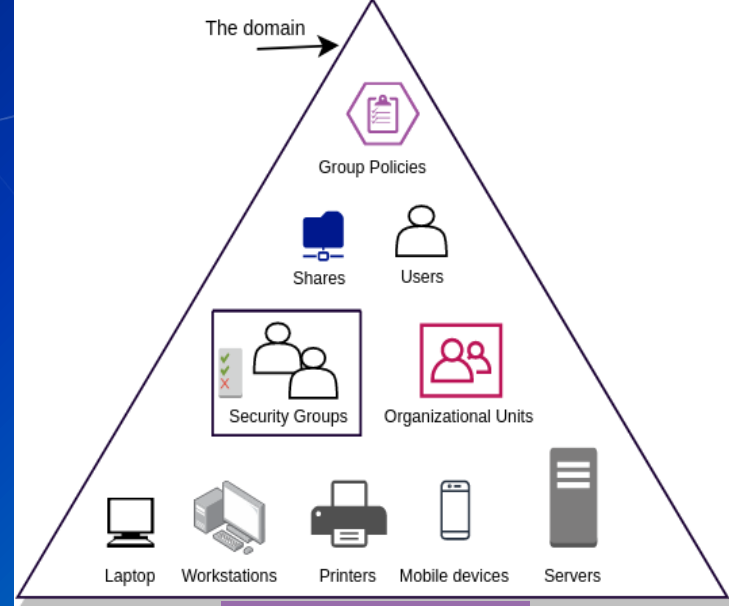
Marketing and Sales OUs have separate policies and administrative controls

# Confused? TL;DR so far:

- 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

# Active Directory - Trees

- Case study: Microsoft Corporation
- Active Directory:
  - Domain – database objects, users, computers...
  - Domain Tree – collection of domains sharing contiguous DNS namespace
- Each subdomain can be used to further **organize** the objects associated with Microsoft
- We use trees to help with the logical management of the domain
- Maintains SSO + trust relationships



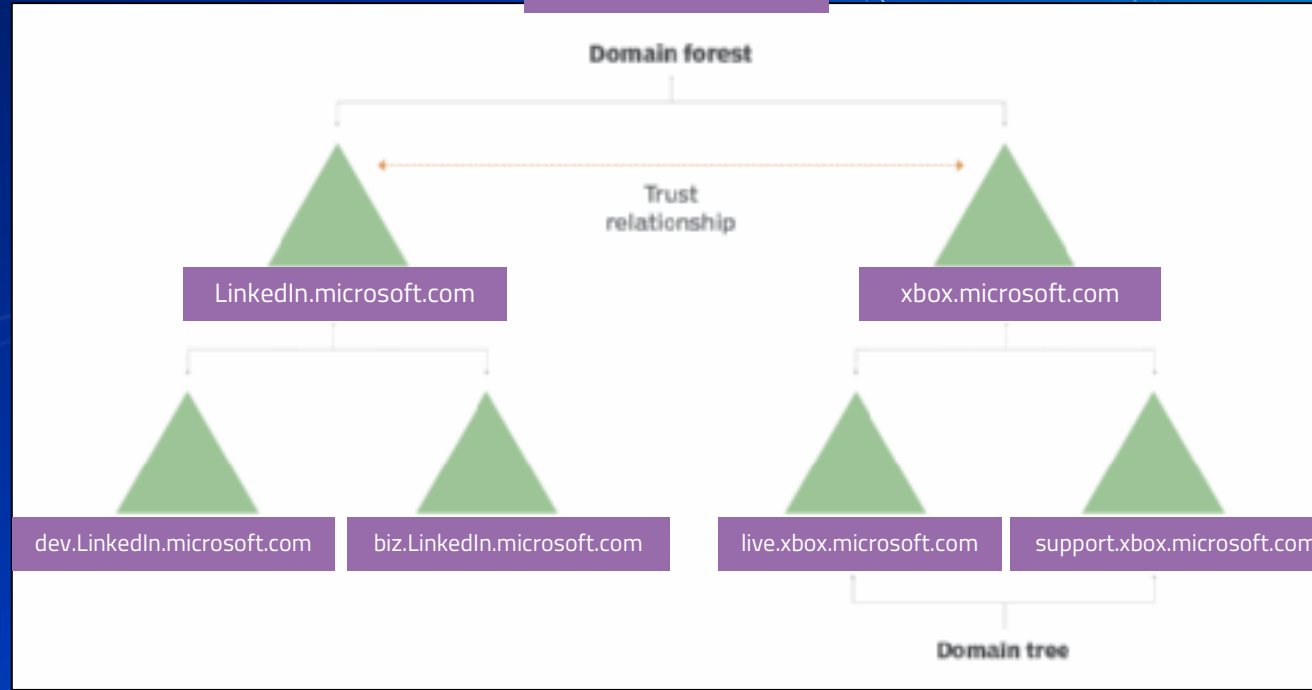
microsoft.com

support.microsoft.com

dev.microsoft.com

# Active Directory - Forests

- 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



**QUESTIONS?**

# Break

Please return in 10 mins

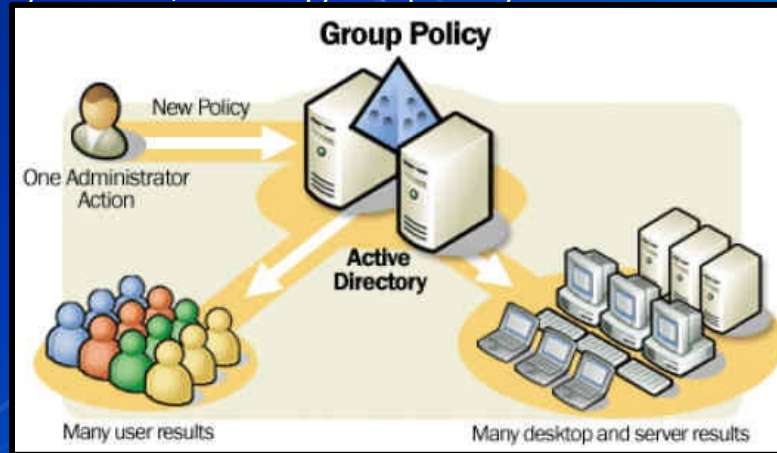


# Agenda

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

# AD - 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 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



# Group Policy Key Terms

## ■ Enforced

- Can not be overwritten by other policy

## ■ Linked

- Link policy to specific OU

## ■ Filtering

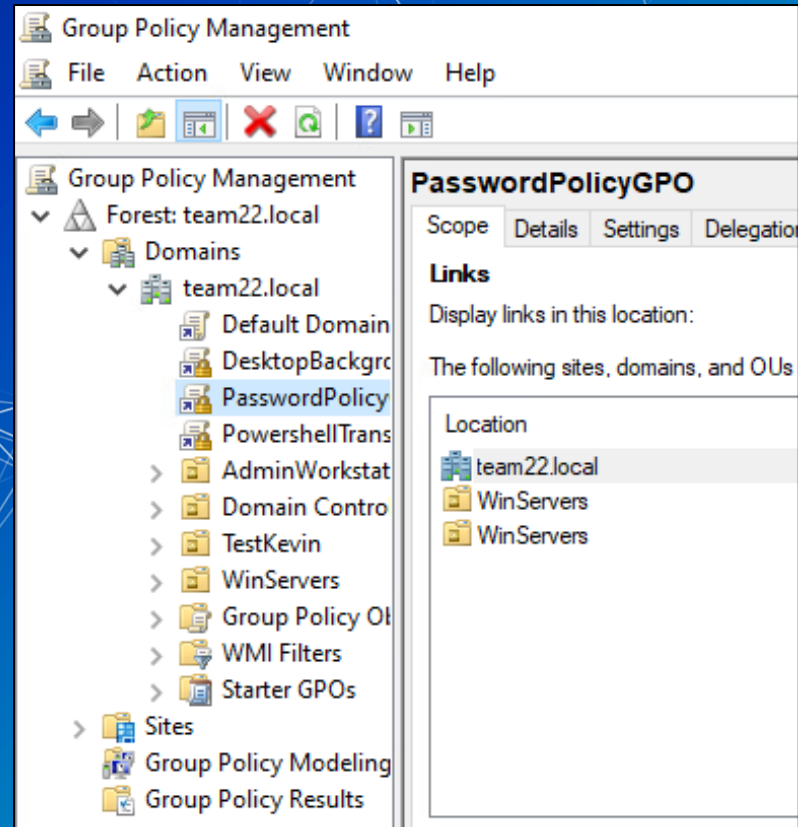
- Can choose to apply Group policy to objects that meet criteria
  - < 8GB RAM

## ■ Group Policy Object (GPO)

- A set of rules that can be applied to any object

# Multiple Group Policies

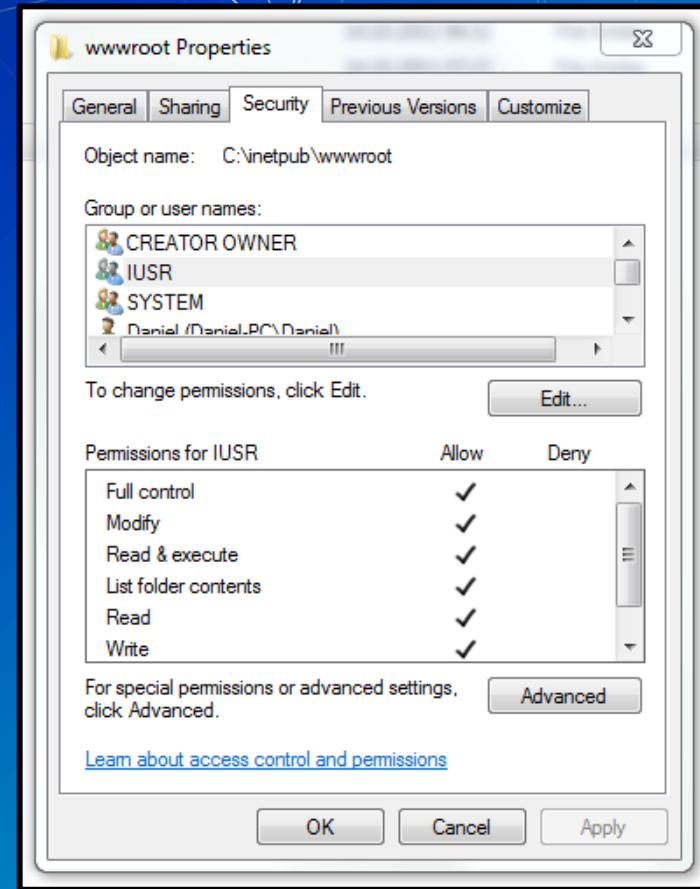
- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group
- **Group policies can be applied to any domain object**
  - Users, Computers, Groups, OUs





# File Permissions

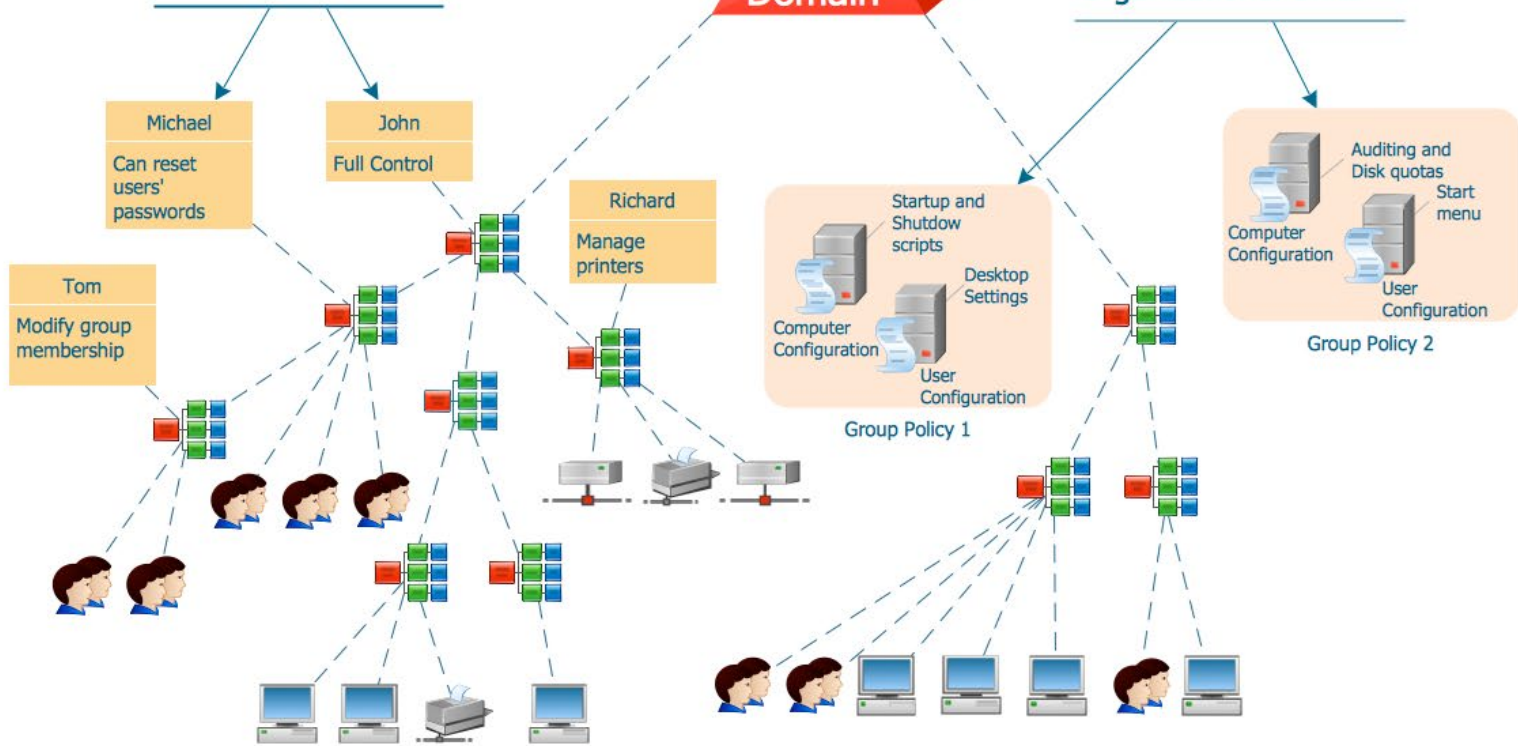
- Can be set on individual files, folders, network shares, hard drives
- Can specify who has read, write, or modify permissions
- File permissions can be inherited from containing folder
- Ex) Can share whole folder instead of every file
- Can be set using group policy and Active Directory









Tasks can be easily delegated

Group Policies applied to Users, Groups or Organizational Units

Domain



Legend

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



# Agenda

1. Windows Systems Information
2. Install Server Experience
3. Services
  - a. IAM
4. Active Directory
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
  - 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

```
PowerShell_transcript.HAWKEYE.OnrOy3IS.20200914184515 - Notepad
File Edit Format View Help
*****
Windows PowerShell transcript start
Start time: 20200914184515
Username: NIMITZ\SYSTEM
RunAs User: NIMITZ\SYSTEM
Configuration Name:
Machine: HAWKEYE (Microsoft Windows NT 10.0.17763.0)
Host Application: powershell.exe
Process ID: 5724
PSVersion: 5.1.17763.1007
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.1007
BuildVersion: 10.0.17763.1007
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
ConfigurationName: 1.1.0.1
```

```
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_MACH...ions\Extensions:String) [New-ItemProperty],
UnauthorizedAccessExcep
+ 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

# 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