Microsoft

UBNetDef, Fall 2022
Week 4
Griffin Refol

Learning Goals

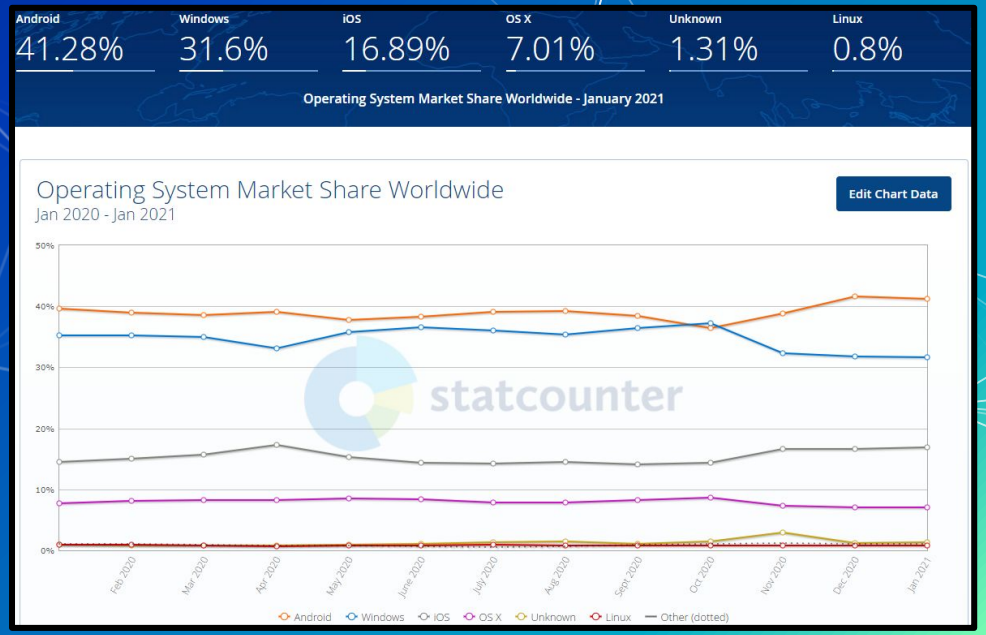
- Understand the difference between Server Desktop and Server Core
- Identify the elements of an Active Directory system
- Create and configure group policy objects
- Distinguish between security groups and organizational units

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

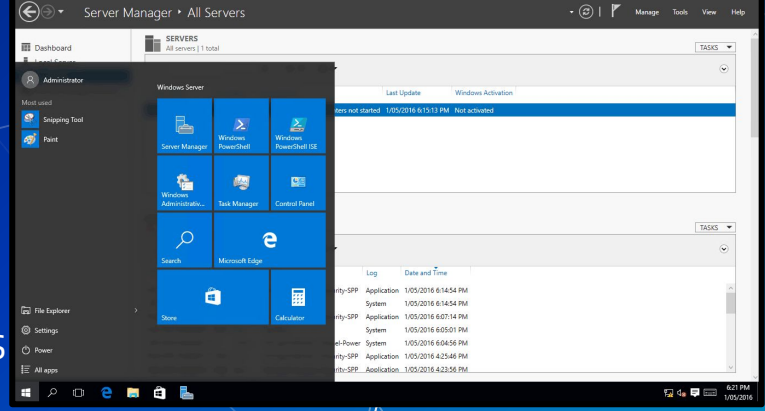
Windows Server vs. Client

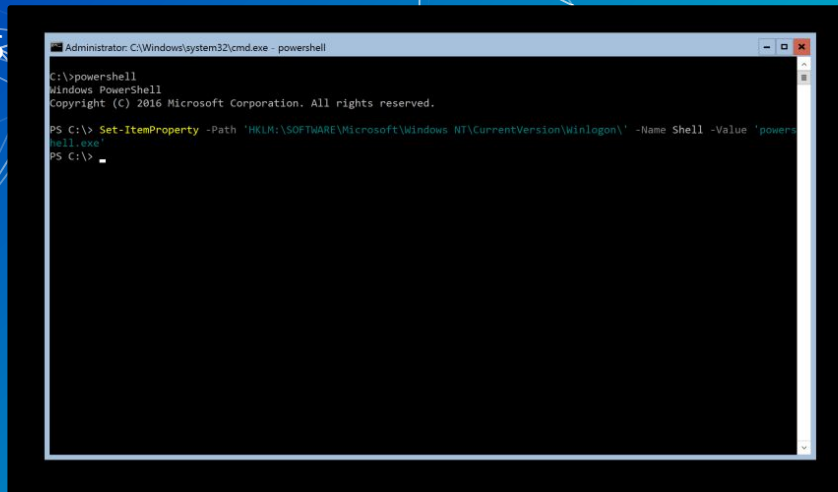
- Windows Client is the tried and true Windows OS that all of you are familiar with
- Windows Server is a OS designed to offer network based services on the Windows Platform



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





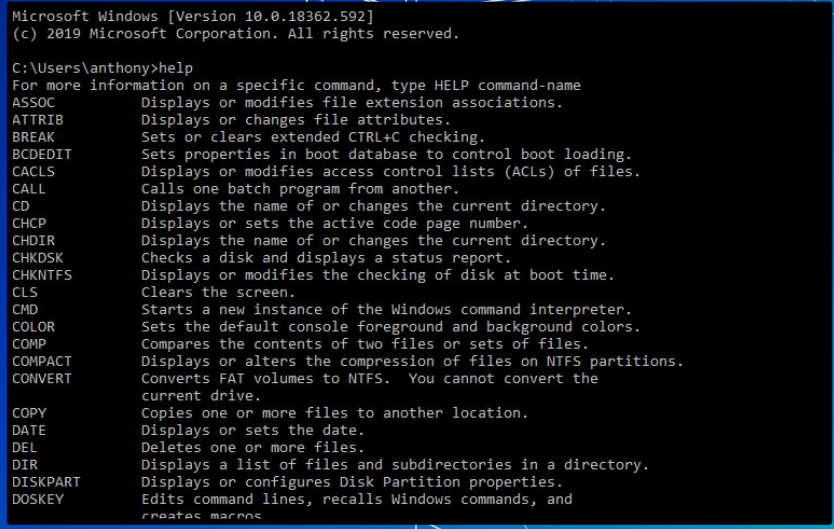
Windows System Level Authority

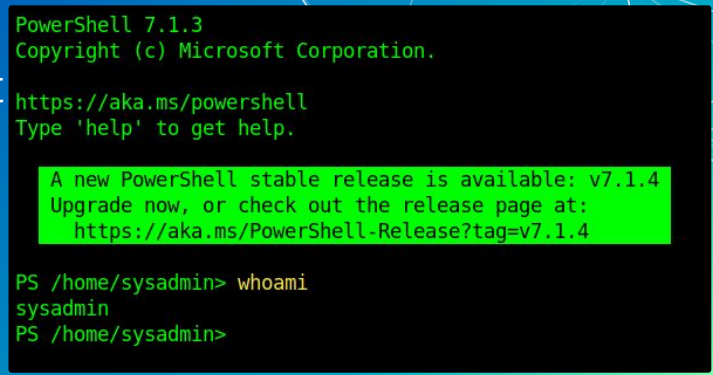
- Special type of account
  - Pre-existing
- Local account (individual per machine)
- Used by the operating system to run Windows related programs
- **Has the highest privileges on the system**
  - User < Administrator < System

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

Command Lines

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



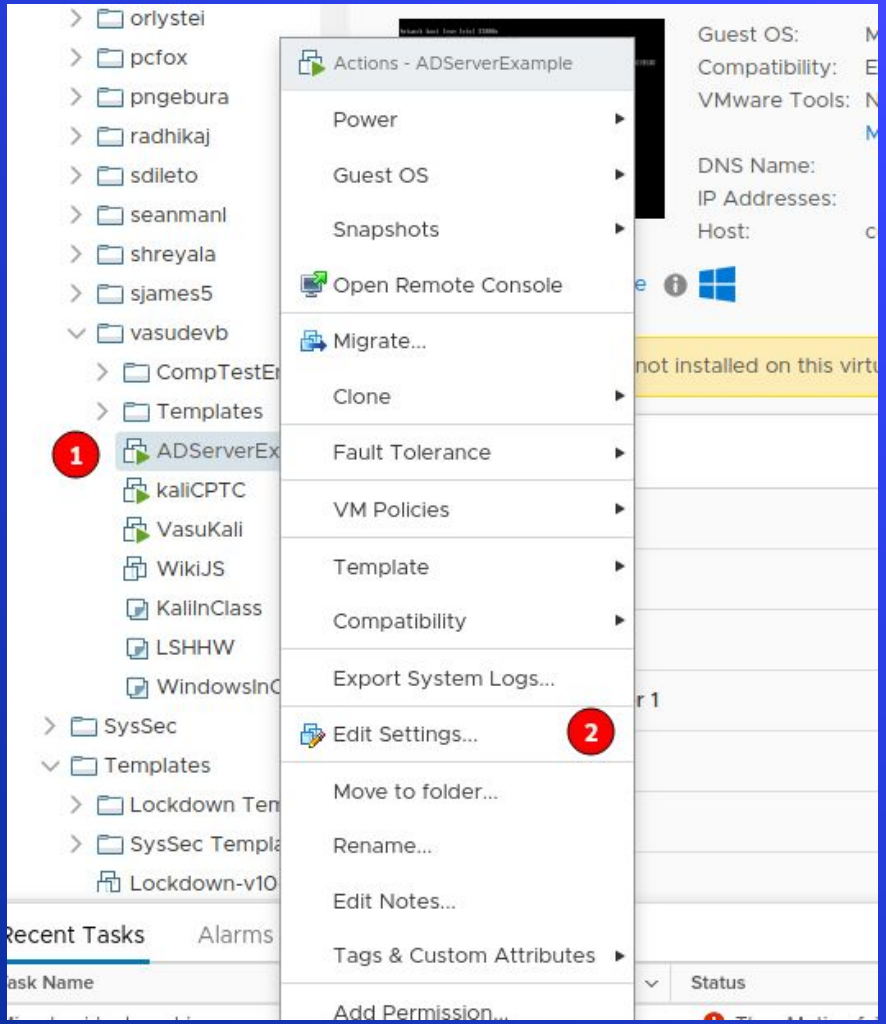


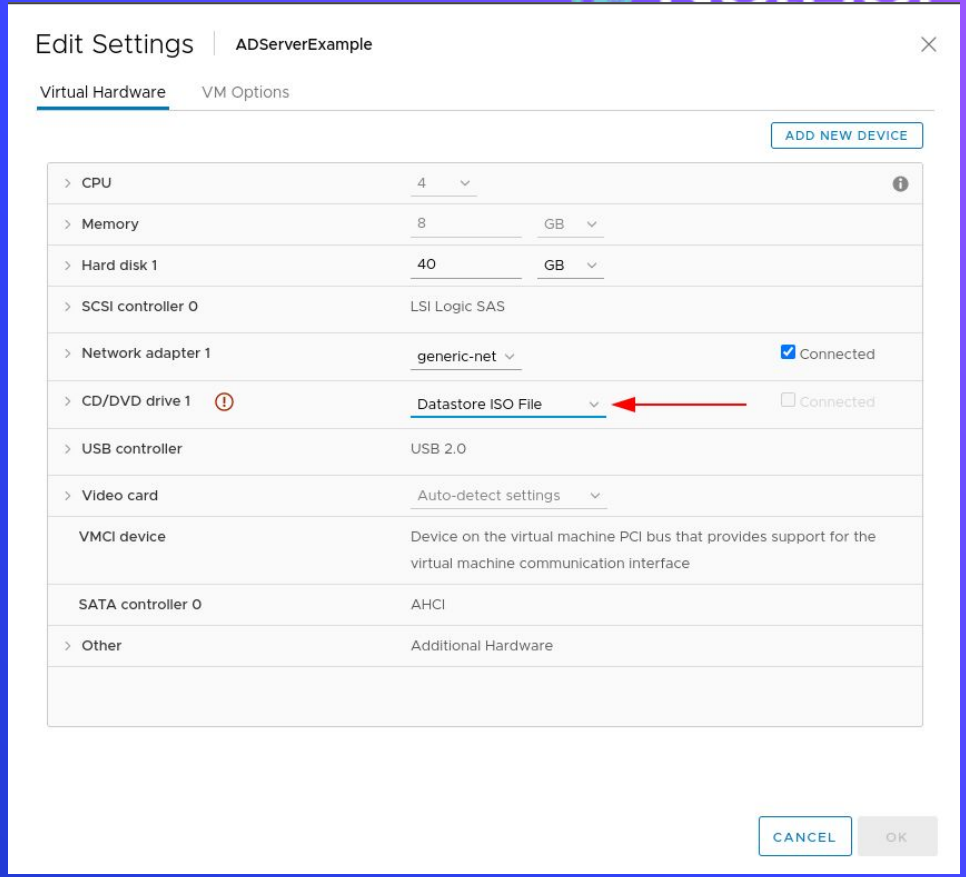
Agenda

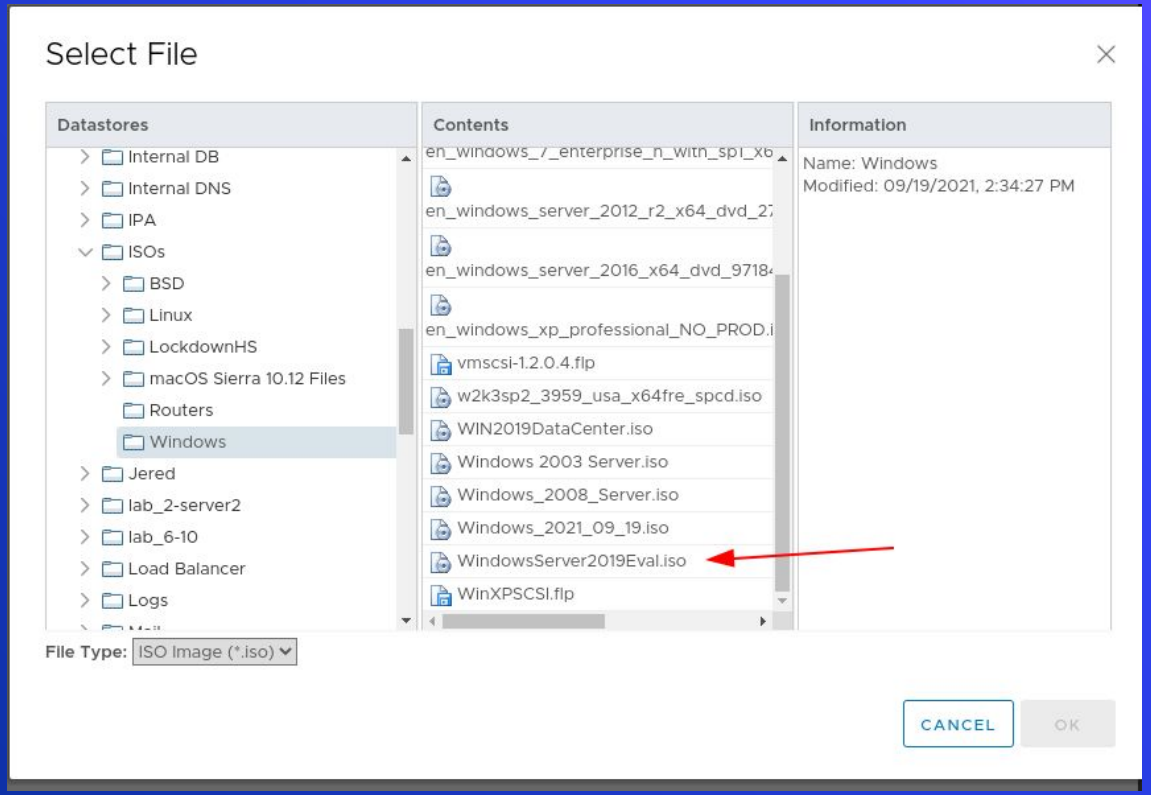
1. Windows Systems Information
2. Install Server Desktop Experience
3. Services
    a. IAM
4. Active Directory
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

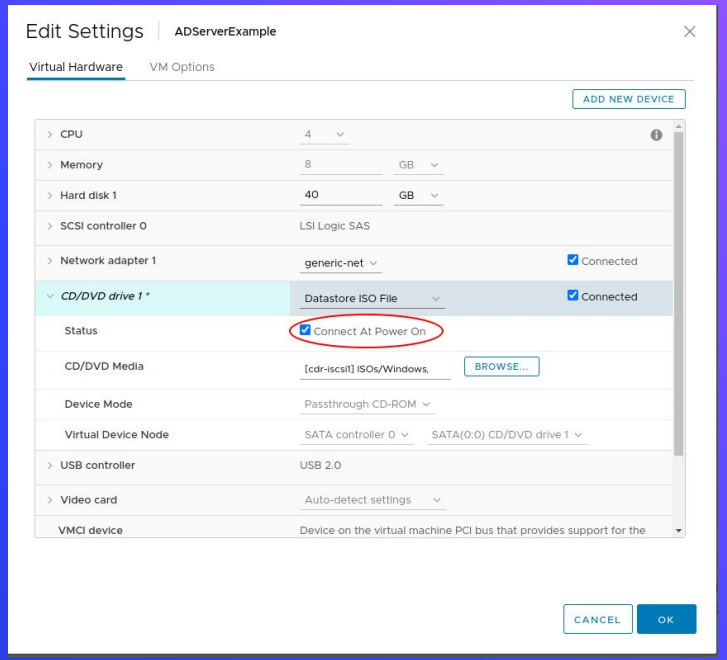
In Class Activity

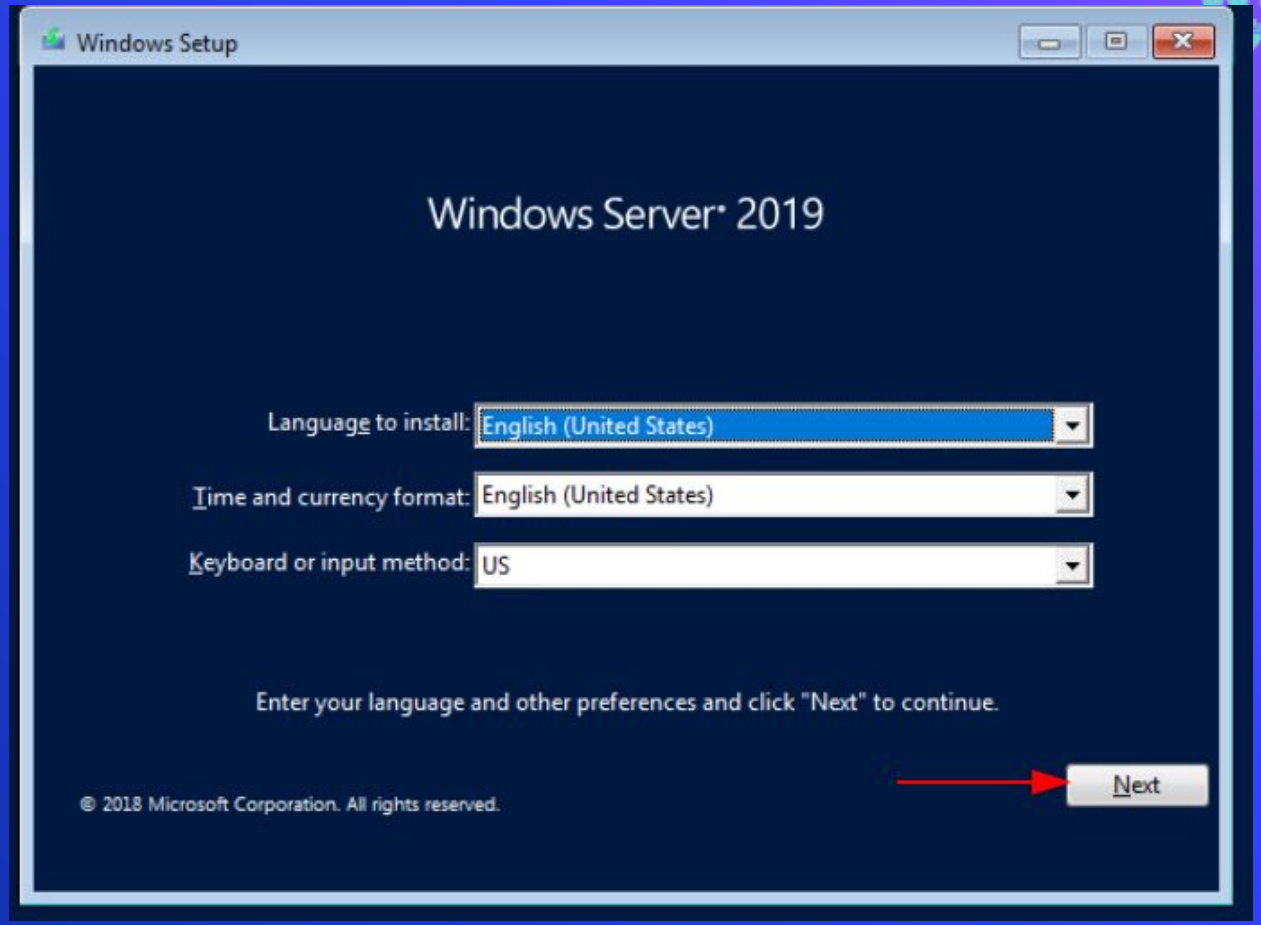
Installing Windows Server

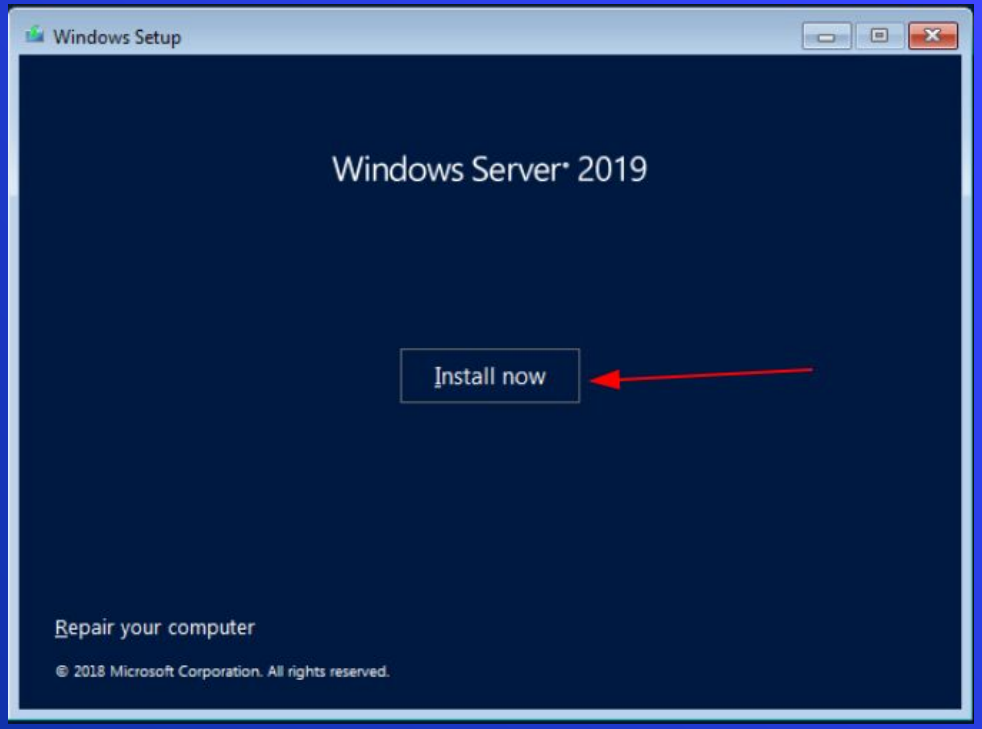

orlystei
pcfox
pngebura
radhikaj
sdileto
seanmanl
shreyala
sjames5
vasudevb
CompTestEr
Templates
ADServerEx
kaliCPTC
VasuKali
WikiJS
KaliInClass
LSHHW
WindowsInC
SysSec
Templates
Lockdown Tem
SysSec Templa
Lockdown-v10
1
Actions - ADServerExample
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
2
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Guest OS:
Compatibility:
VMware Tools:
DNS Name:
IP Addresses:
Host:
not installed on this virtu
r 1
Recent Tasks
Alarms
ask Name
Status

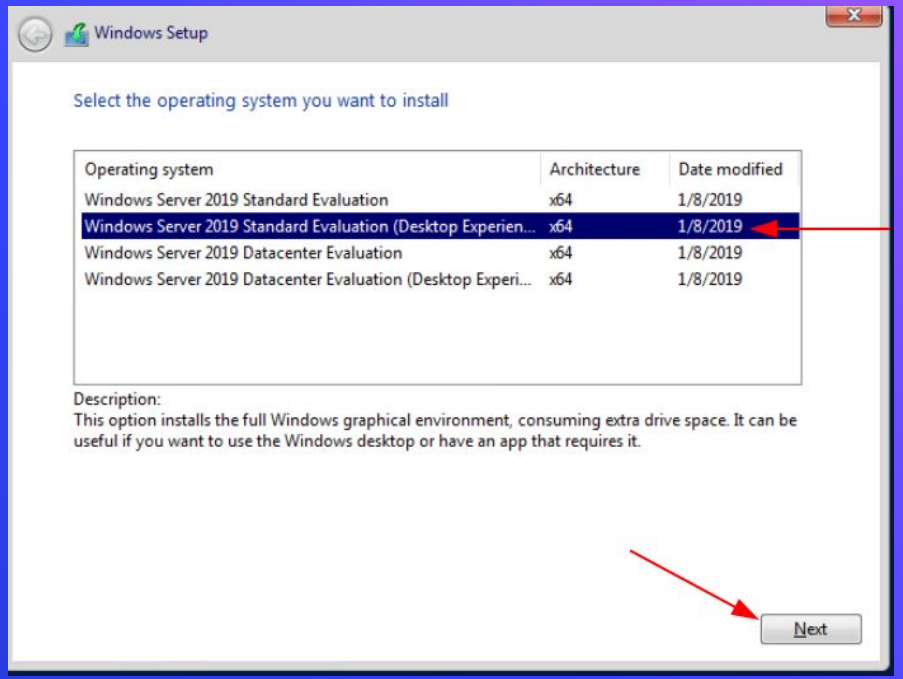

Edit Settings
ADServerExample
Virtual Hardware
VM Options
ADD NEW DEVICE
CPU
4
Memory
8
GB
Hard disk 1
40
GB
SCSI controller 0
LSI Logic SAS
Network adapter 1
generic-net
Connected
CD/DVD drive 1
Datastore ISO File
Connected
USB controller
USB 2.0
Video card
Auto-detect settings
VMCI device
Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
SATA controller 0
AHCI
Other
Additional Hardware
CANCEL
OK

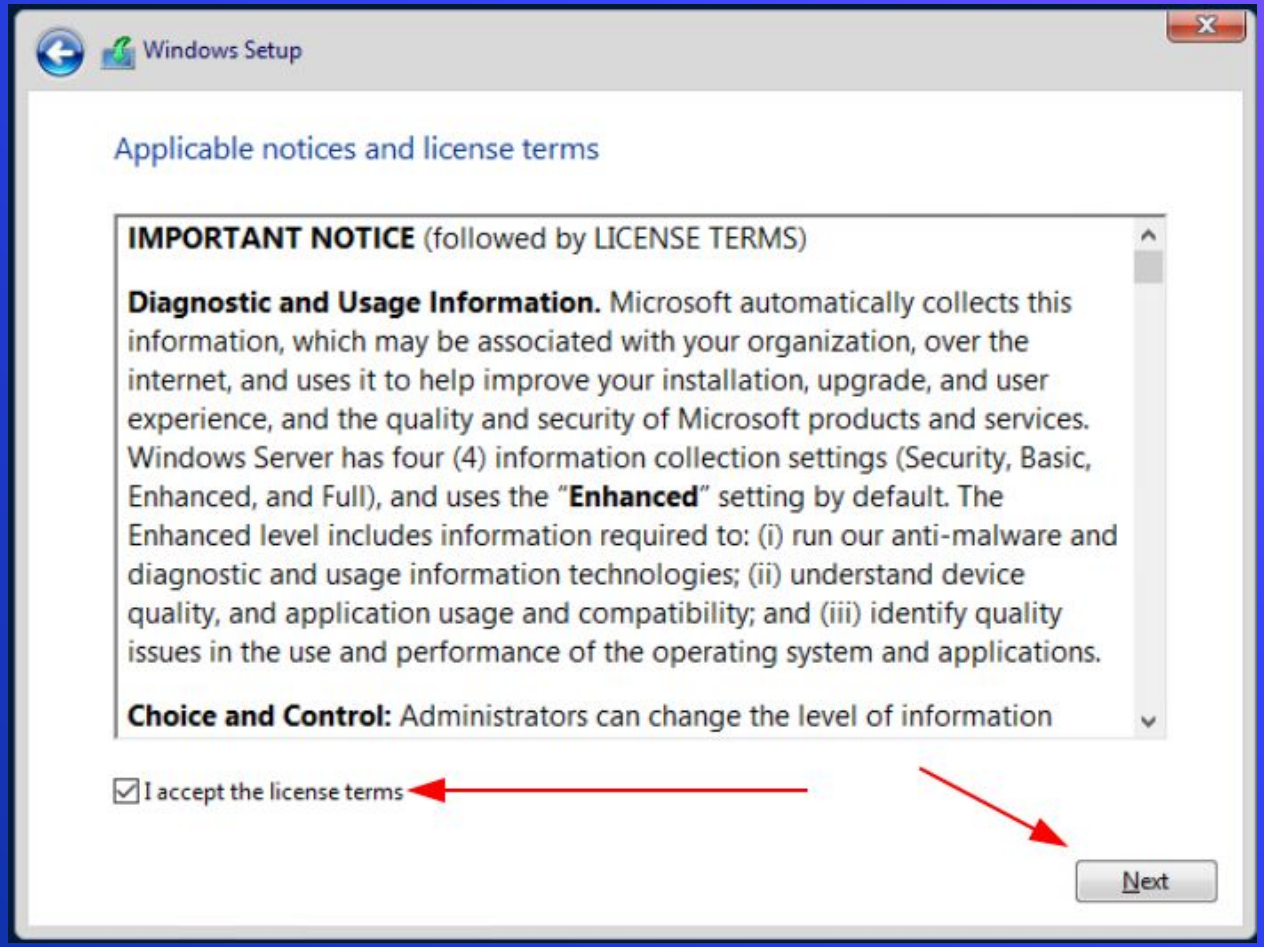

Select File
Datastores
Contents
Information
Internal DB
Internal DNS
IPA
ISOs
BSD
Linux
LockdownHS
macOS Sierra 10.12 Files
Routers
Windows
Jered
lab_2-server2
lab_6-10
Load Balancer
Logs
en_windows_server_2012_r2_x64_dvd_2
en_windows_server_2016_x64_dvd_9718
en_windows_xp_professional_NO_PROD.i
vmscsi-1.2.0.4.flp
w2k3sp2_3959_usa_x64fre_spcd.iso
WIN2019DataCenter.iso
Windows 2003 Server.iso
Windows_2008_Server.iso
Windows_2021_09_19.iso
WindowsServer2019Eval.iso
WinXPSCSI.flp
Name: Windows
Modified: 09/19/2021, 2:34:27 PM
File Type:
ISO Image (*.iso)
CANCEL
OK

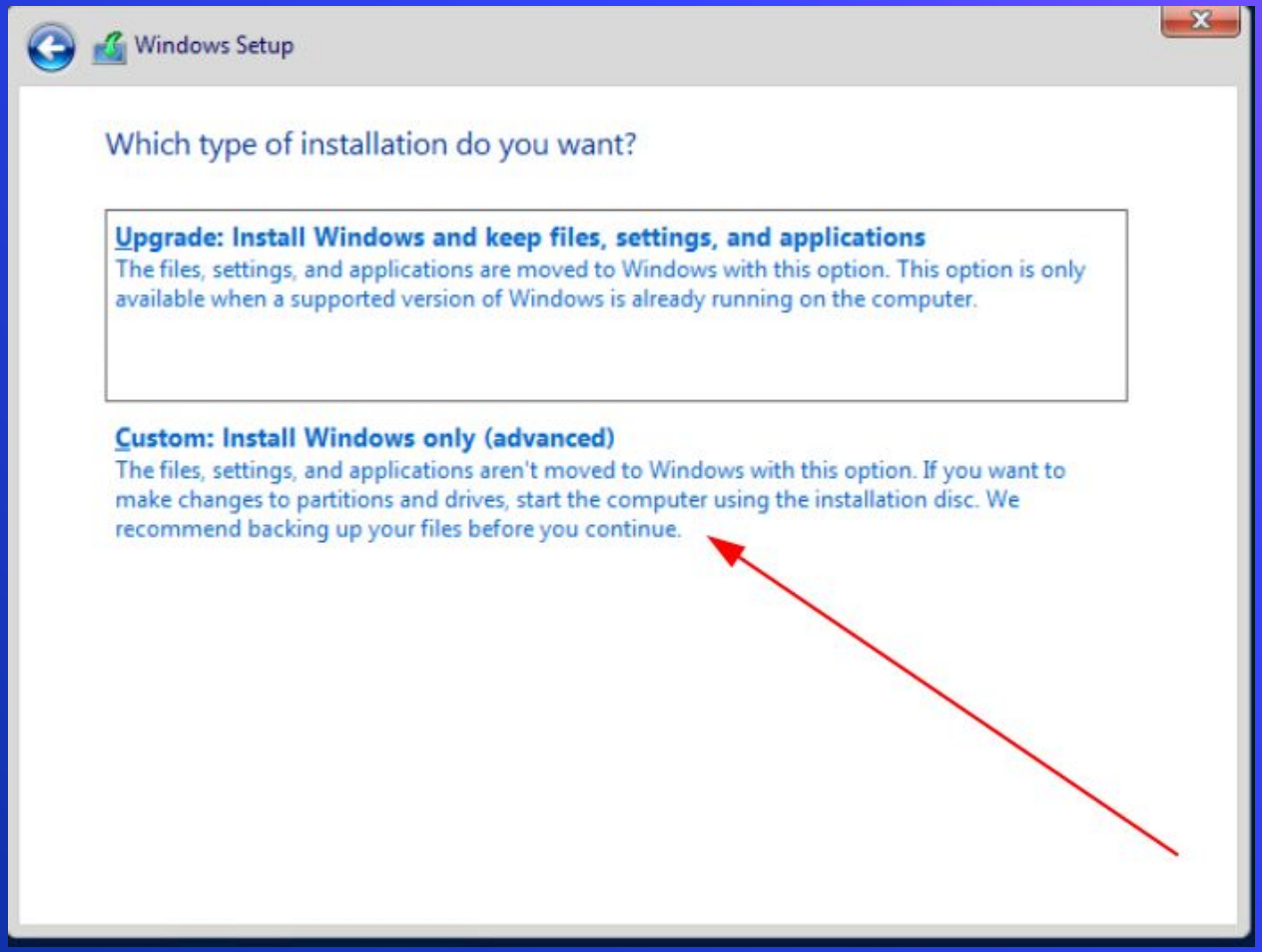

Edit Settings
ADServerExample
Virtual Hardware
VM Options
ADD NEW DEVICE
CPU
4
Memory
8
GB
Hard disk 1
40
GB
SCSI controller 0
LSI Logic SAS
Network adapter 1
generic-net
Connected
CD/DVD drive 1 *
Datastore ISO File
Connected
Status
Connect At Power On
CD/DVD Media
[cdr-iscsi1] ISOs/Windows,
BROWSE...
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

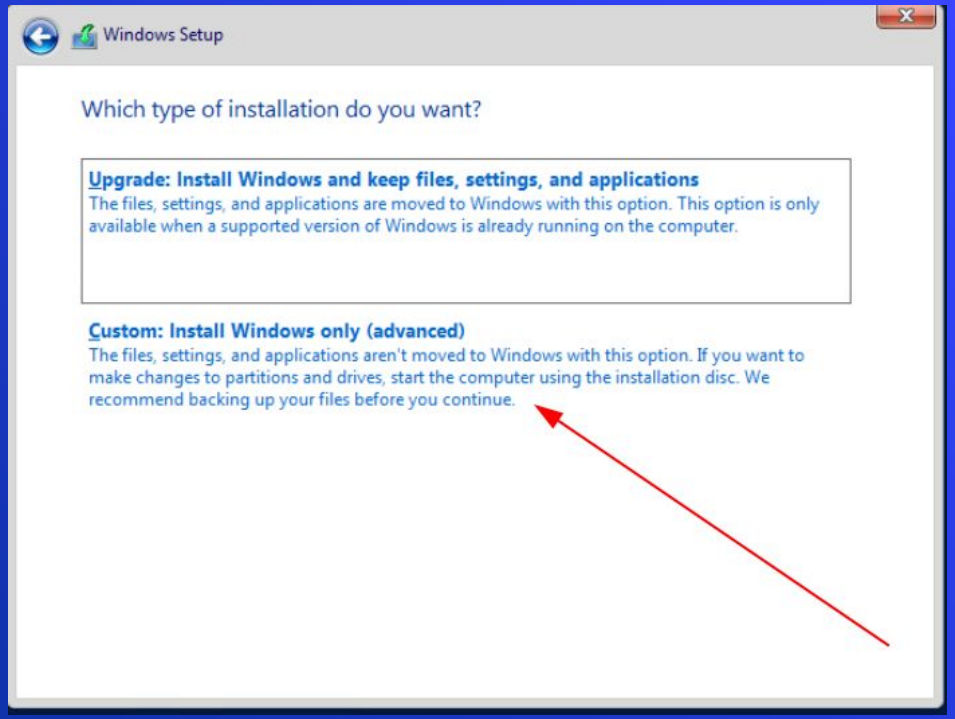

Windows Setup
Windows Server 2019
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2018 Microsoft Corporation. All rights reserved.
Next

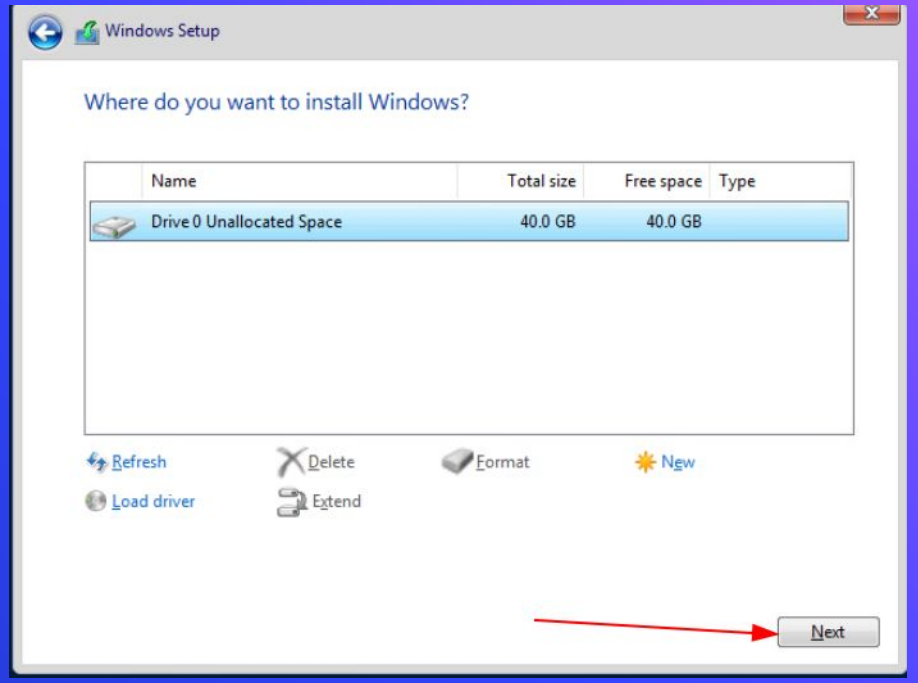

Windows Setup
Windows Server 2019
Install now
Repair your computer
© 2018 Microsoft Corporation. All rights reserved.


Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2019 Standard Evaluation
x64
1/8/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...
x64
1/8/2019
Windows Server 2019 Datacenter Evaluation
x64
1/8/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...
x64
1/8/2019
Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Next


Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
Choice and Control: Administrators can change the level of information
I accept the license terms
Next


Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.


Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

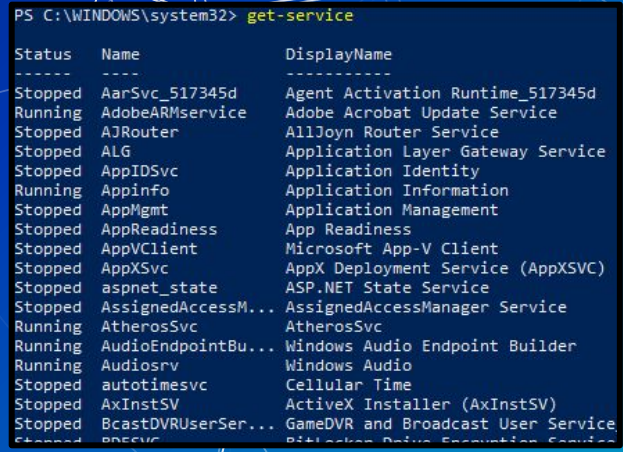

Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
40.0 GB
40.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next

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

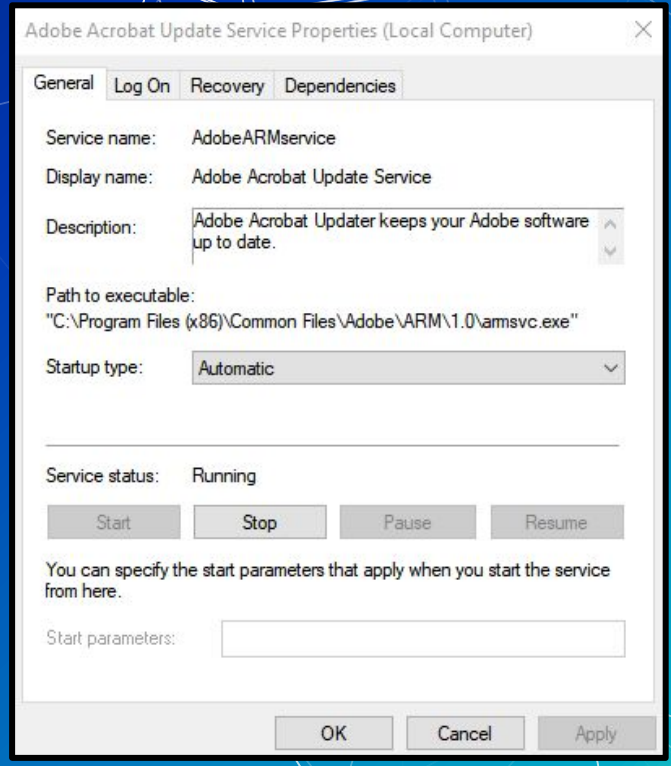
Services and Processes

- 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



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



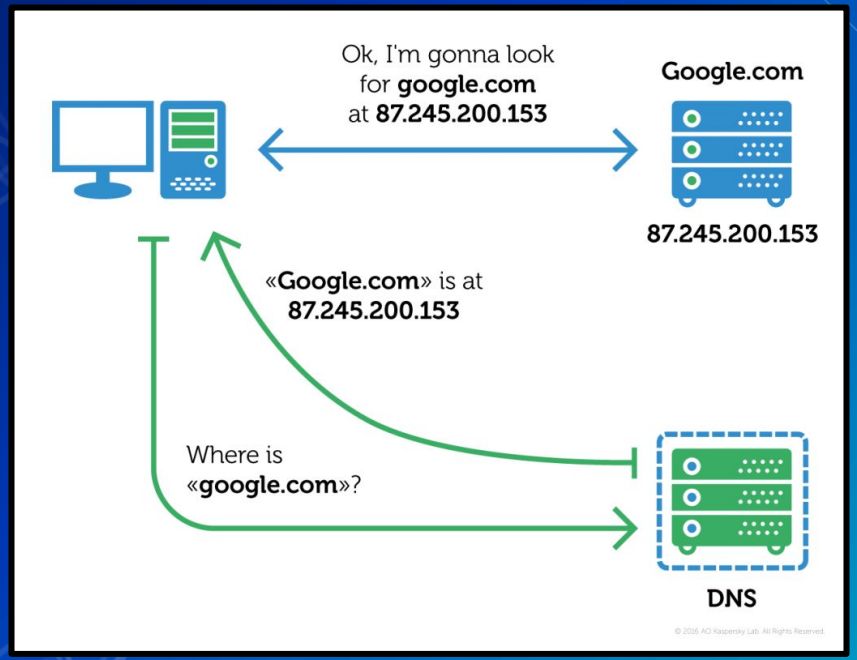

```
PS C:\WINDOWS\system32> Restart-Service Spooler -v
VERBOSE: Performing the operation "Restart-Service" on target "Print Spooler (Spooler)".
```

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

DNS

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



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
  - Never trust a machine by virtue of its IP address
  - Always verify the user's identity and level of access
- Multi-Factor Authentication (MFA) components:
  - Something the user knows
  - Something the user has
  - Something the user is
- Case in point: vCenter, UBLearns

IAM

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

QUESTIONS?

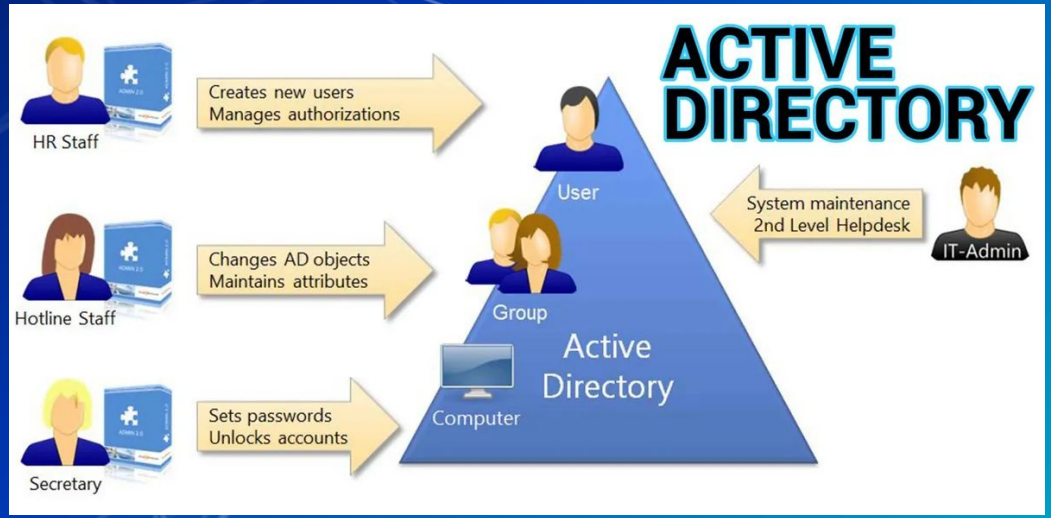
IAM can be complicated, but powerful.

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

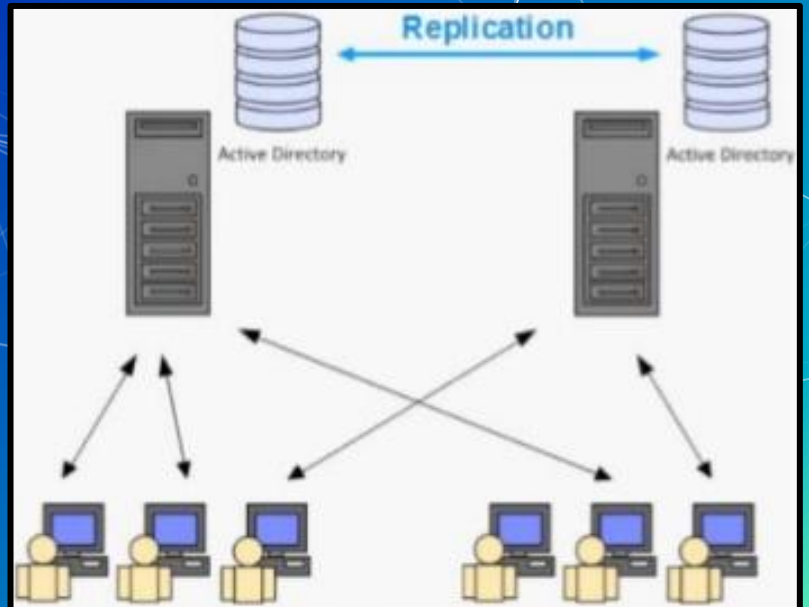


Components of Active Directory (AD)

- 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.

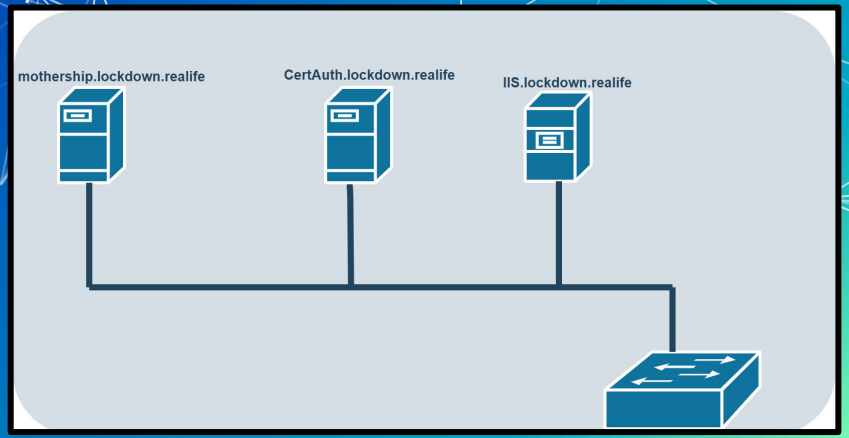
Domain Controllers (DCs)

- Can have multiple Domain Controllers to have redundancy or server load balancing
- Handles authentication requests for the domain
  - Also runs the DNS
  - And more!



AD <3 DNS

- AD absolutely requires DNS to function.
  - AD communicates with computers over domain names, not IP addresses.
  - IP's can change.
  - Computer names are unique per domain.
- Domain controllers (that run AD) also usually* serve as the local AD DNS & DHCP server.
  - DHCP automatically assigns IPs.



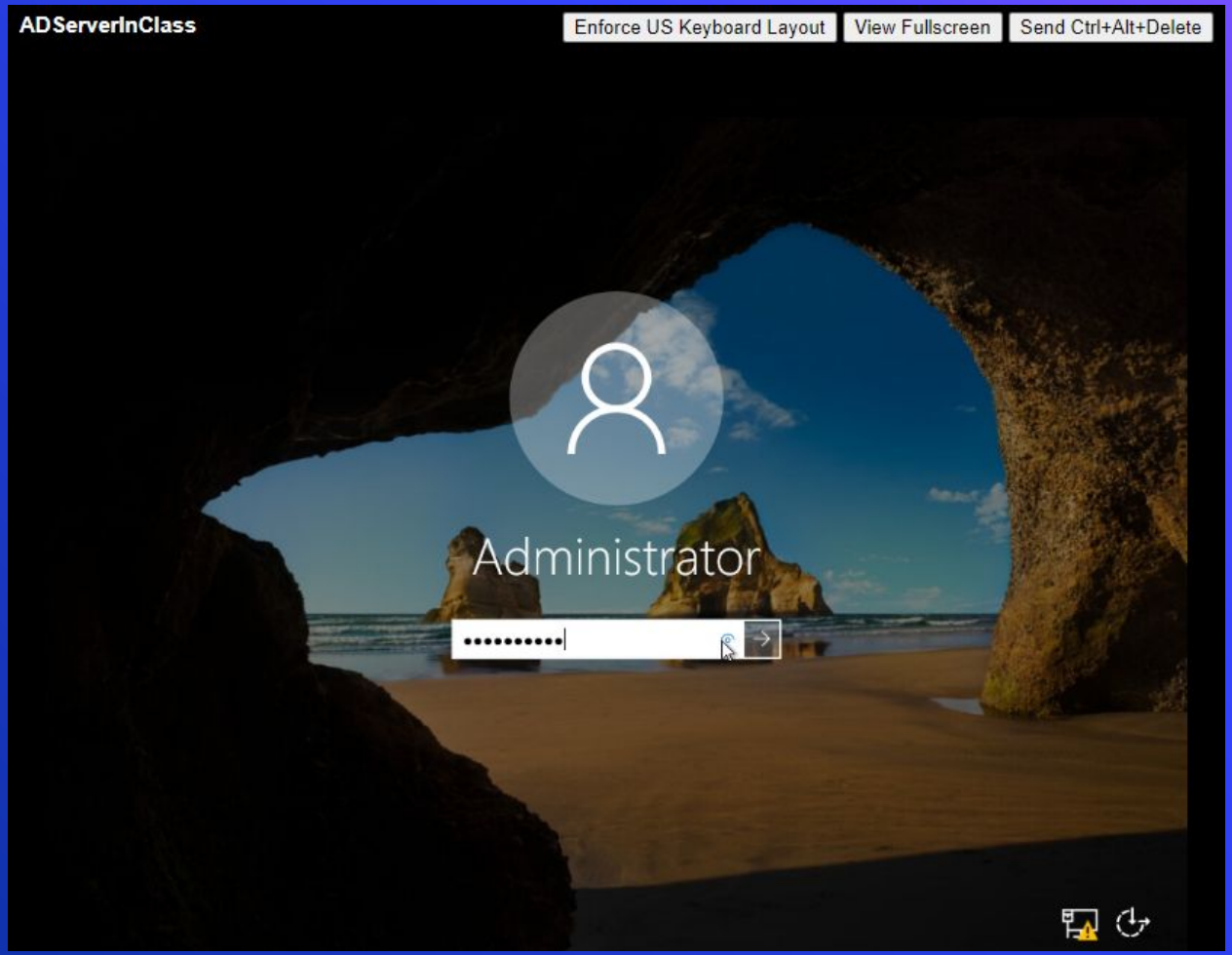
Agenda

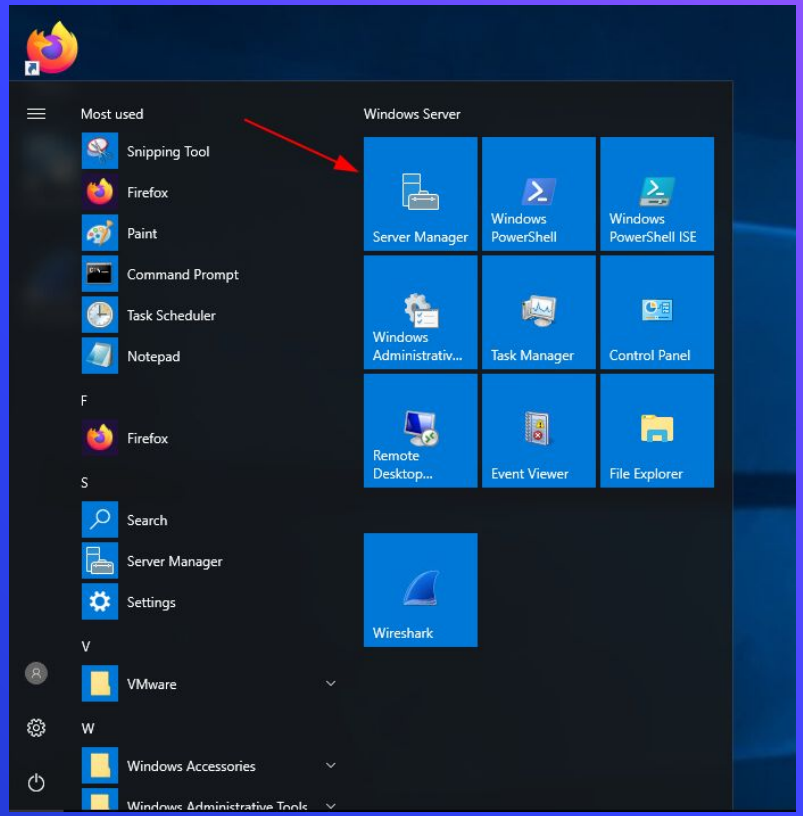
1. Windows Systems Information
2. Install Server Experience
3. Services
   a. IAM
4. Active Directory
5. Install AD Service
6. Components of an AD Service
7. Group Policy
8. Security Considerations
9. HW

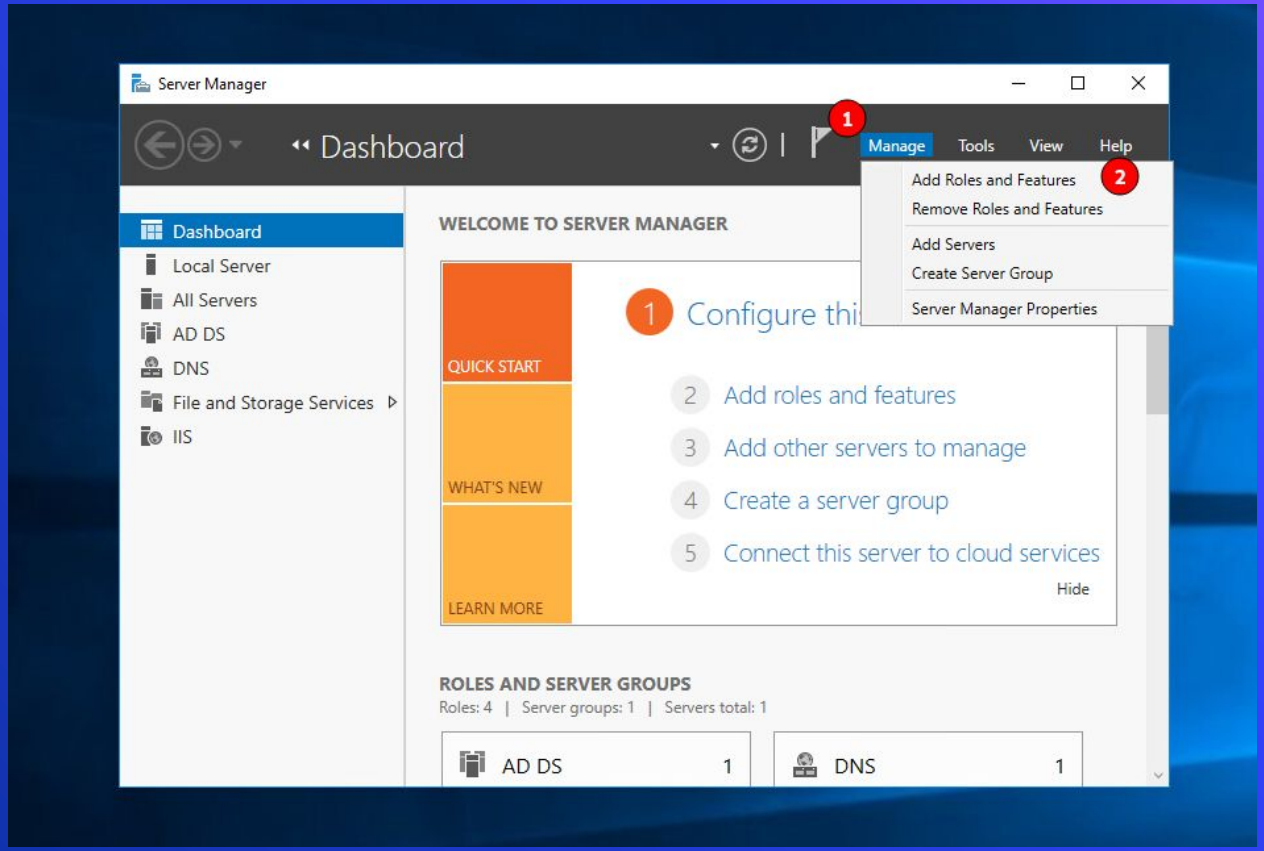
In Class Activity

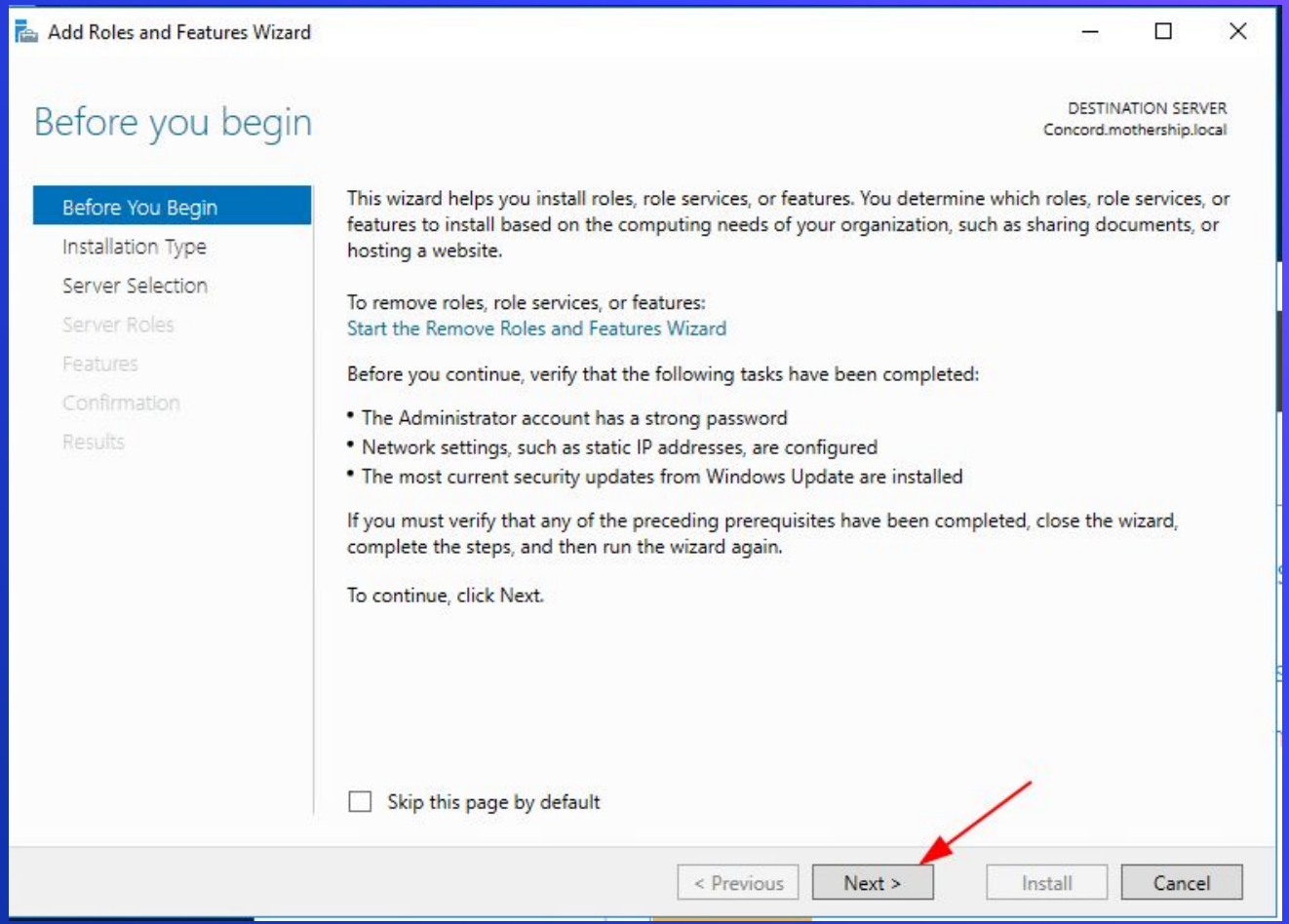
Setting up DNS

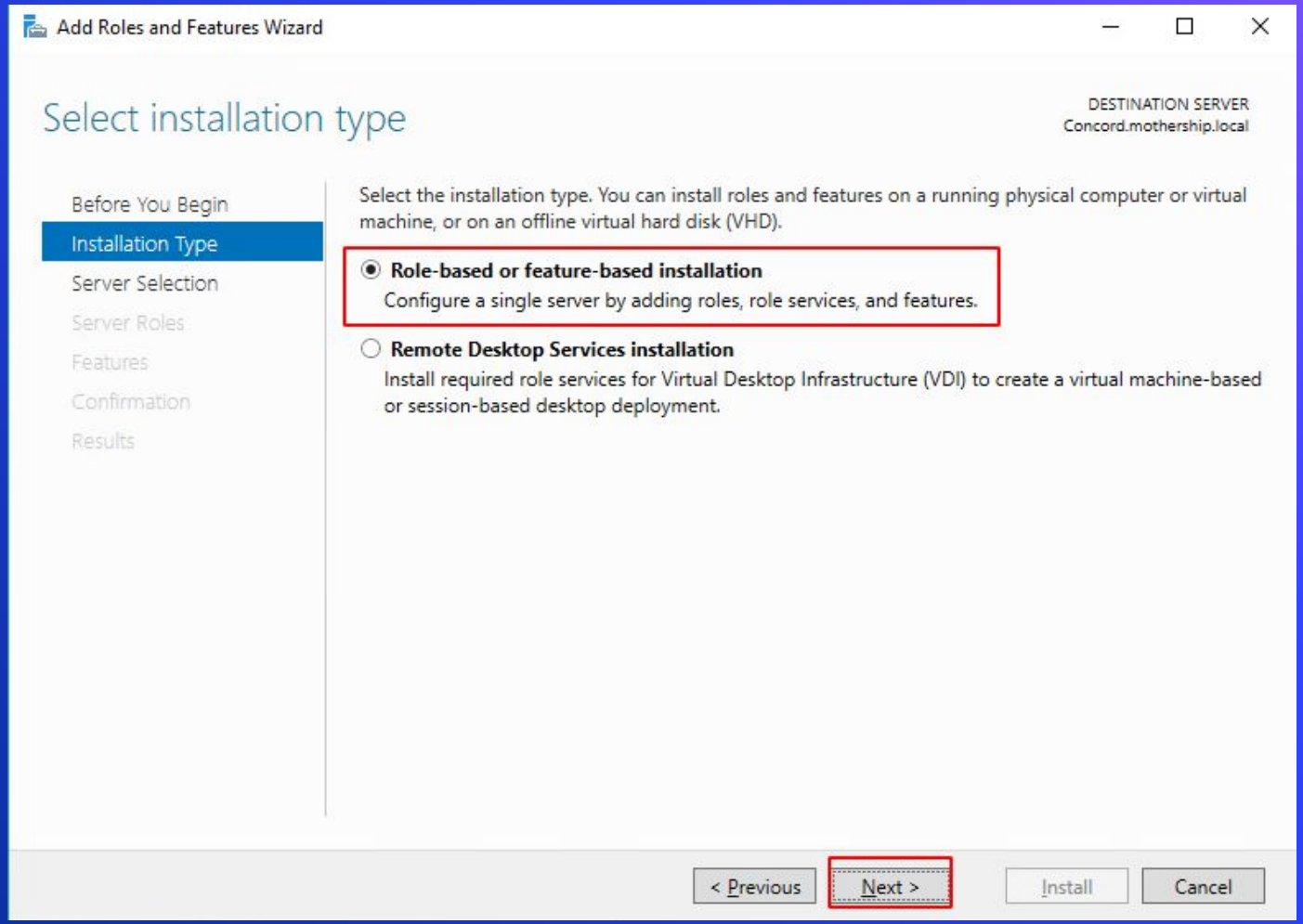

ADServerInClass
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Press Ctrl+Alt+Delete to unlock.
5:22
Thursday, September 23

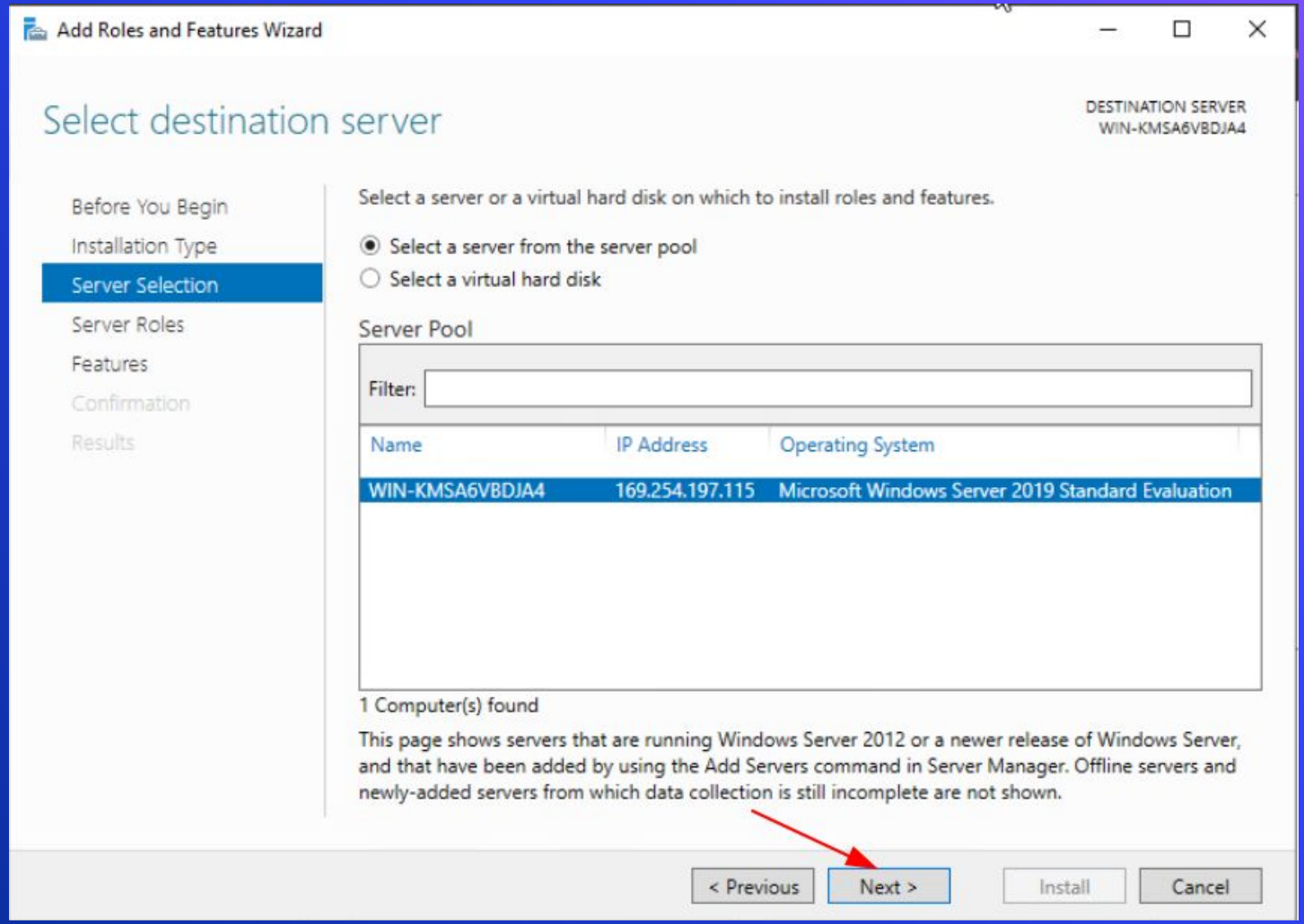

ADServerInClass
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Administrator

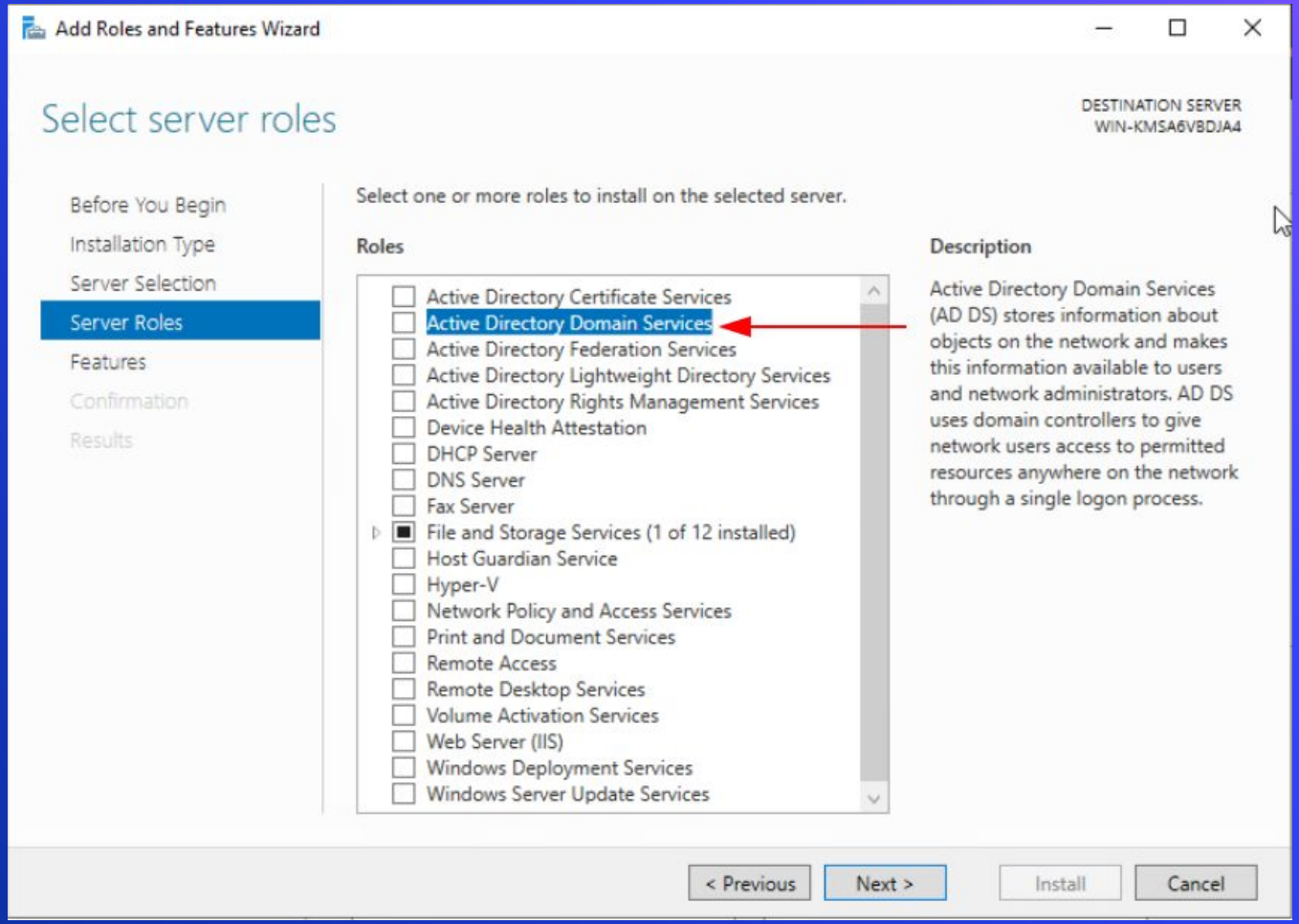

Most used
Snipping Tool
Firefox
Paint
Command Prompt
Task Scheduler
Notepad
F
Firefox
S
Search
Server Manager
Settings
V
VMware
W
Windows Accessories
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
Wireshark

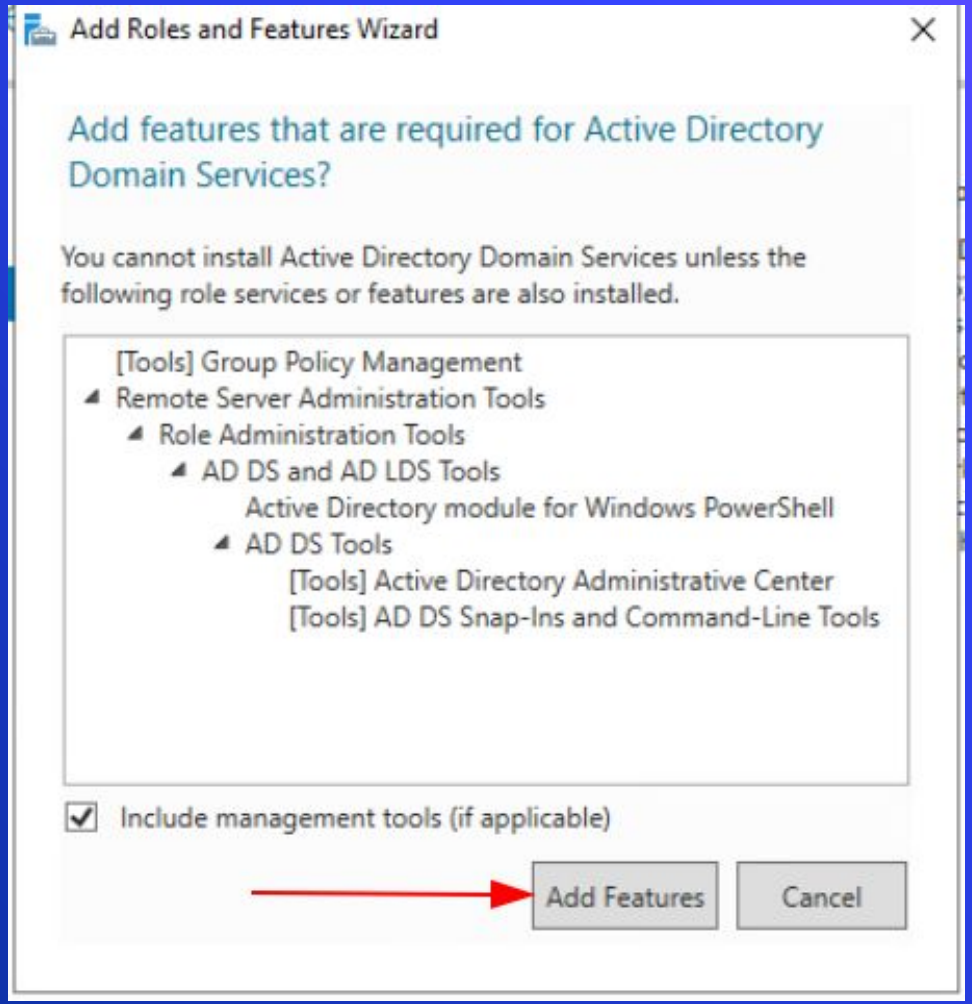

Server Manager
Dashboard
1
Manage
Tools
View
Help
Add Roles and Features
2
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure thi
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

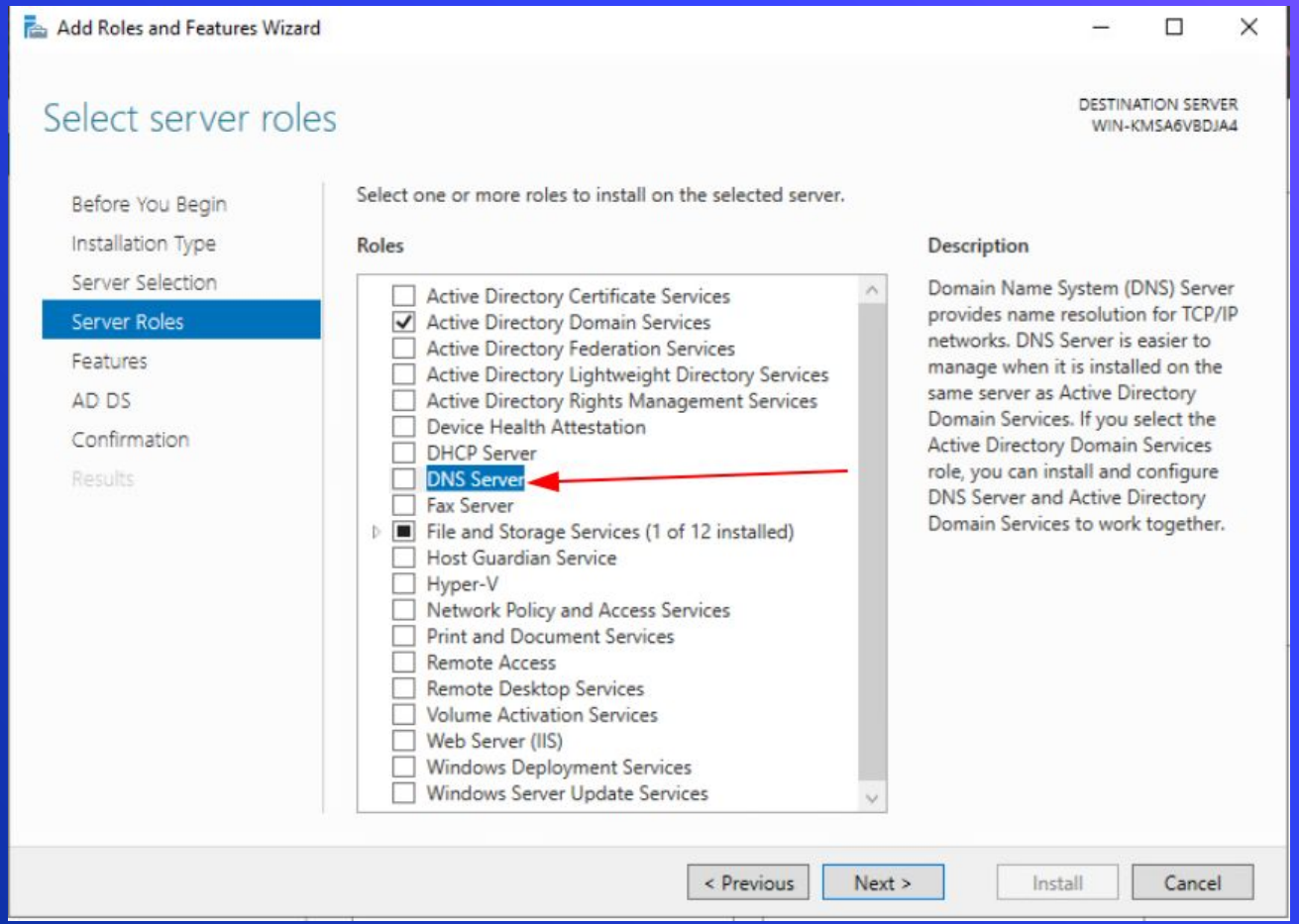

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
Concord.mothership.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features 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

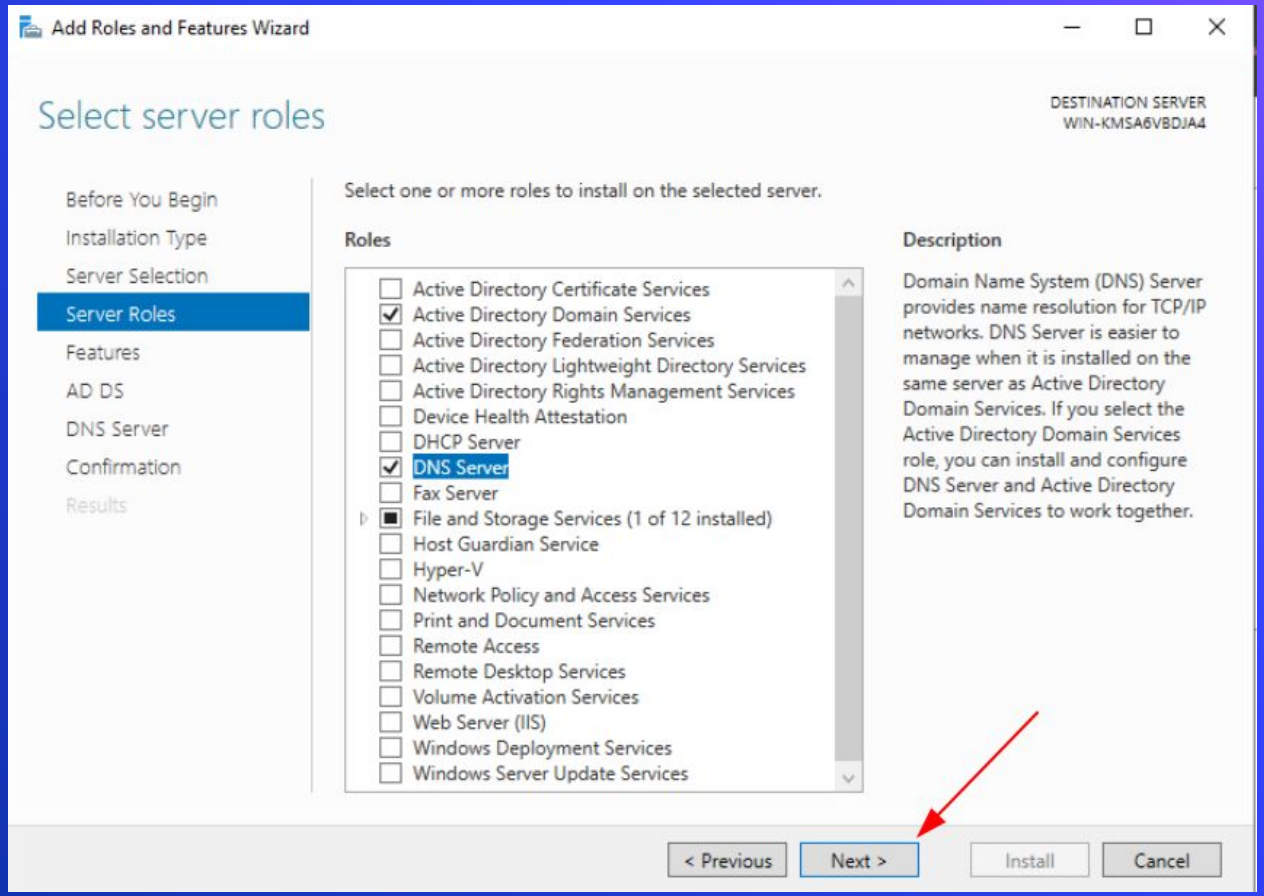

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
Concord.mothership.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual 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.
< Previous
Next >
Install
Cancel

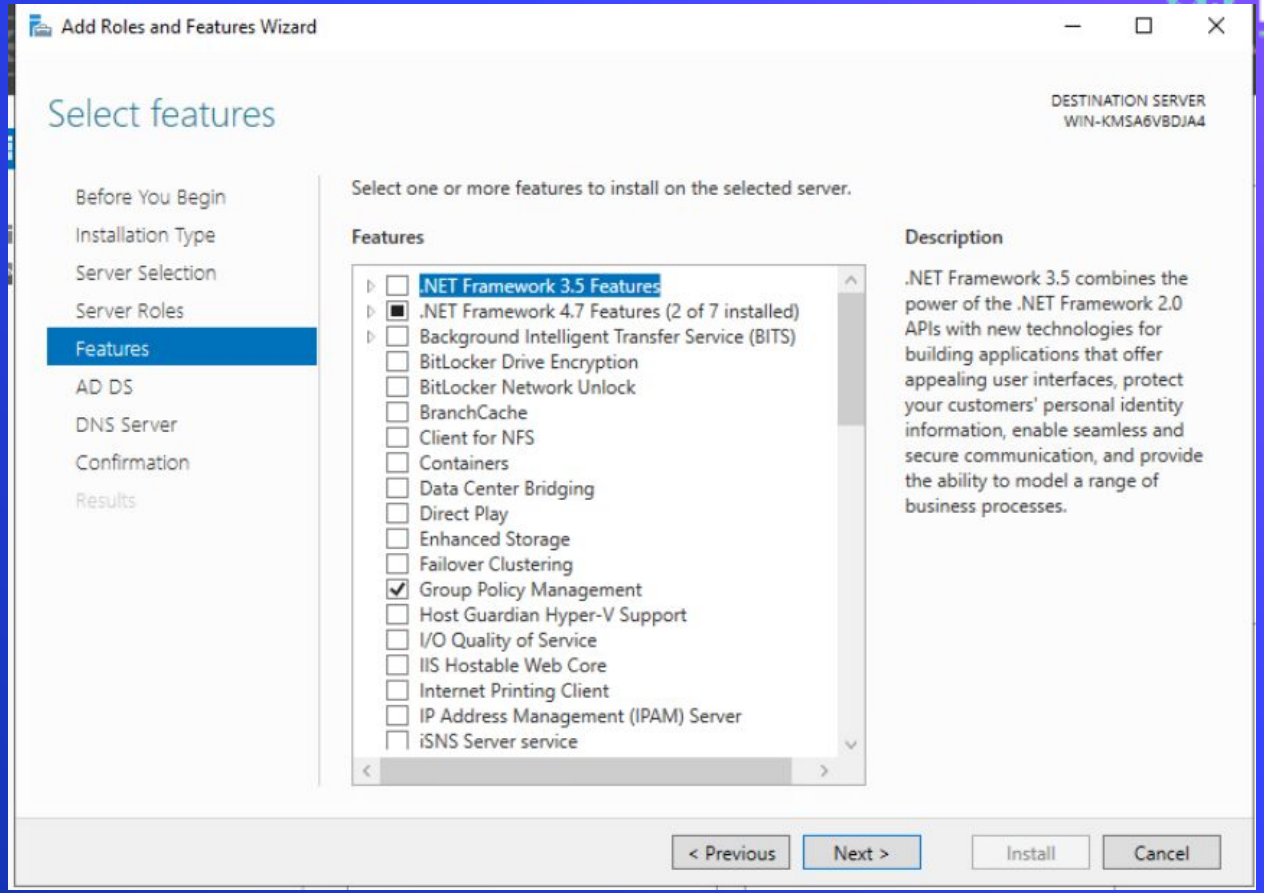

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
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.
< Previous
Next >
Install
Cancel

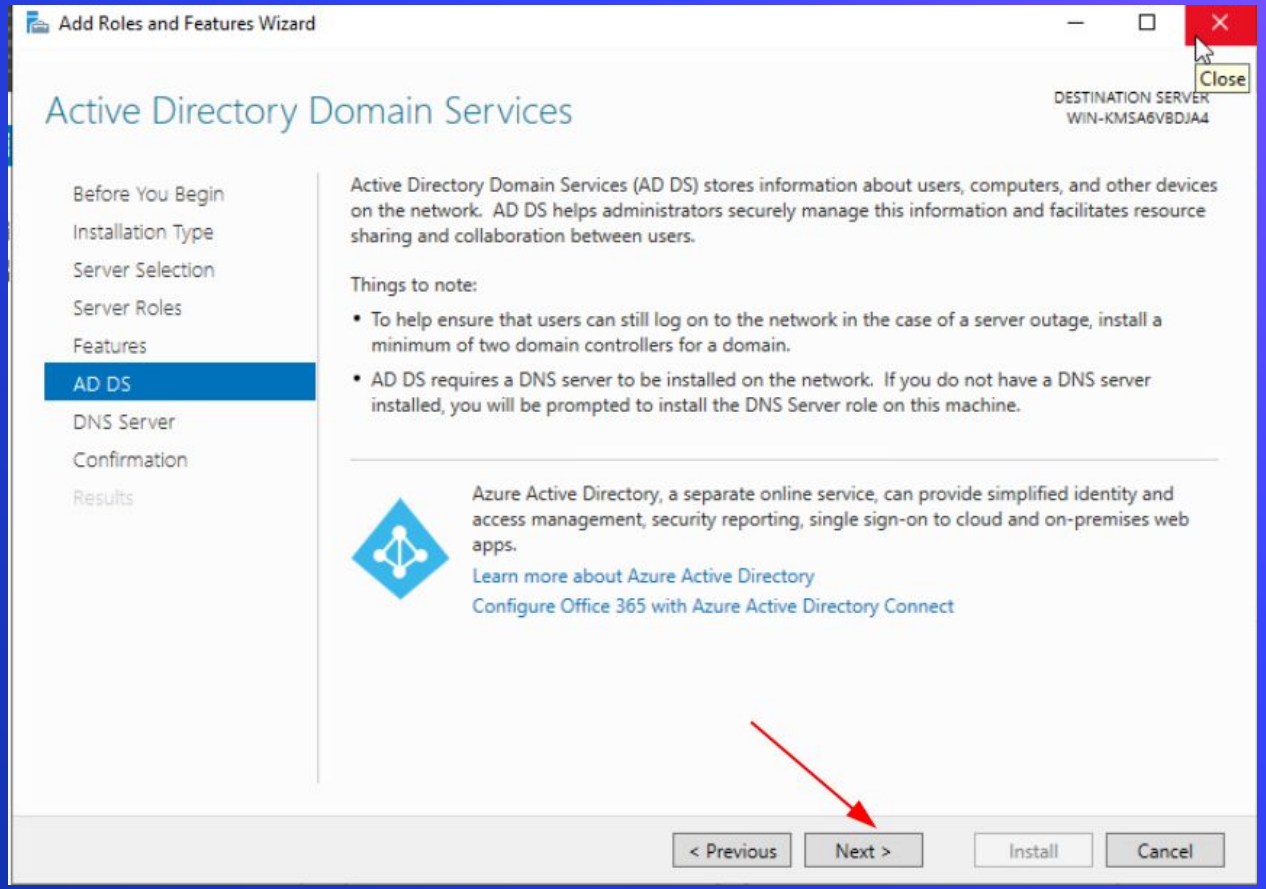

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory 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
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.
< Previous
Next >
Install
Cancel

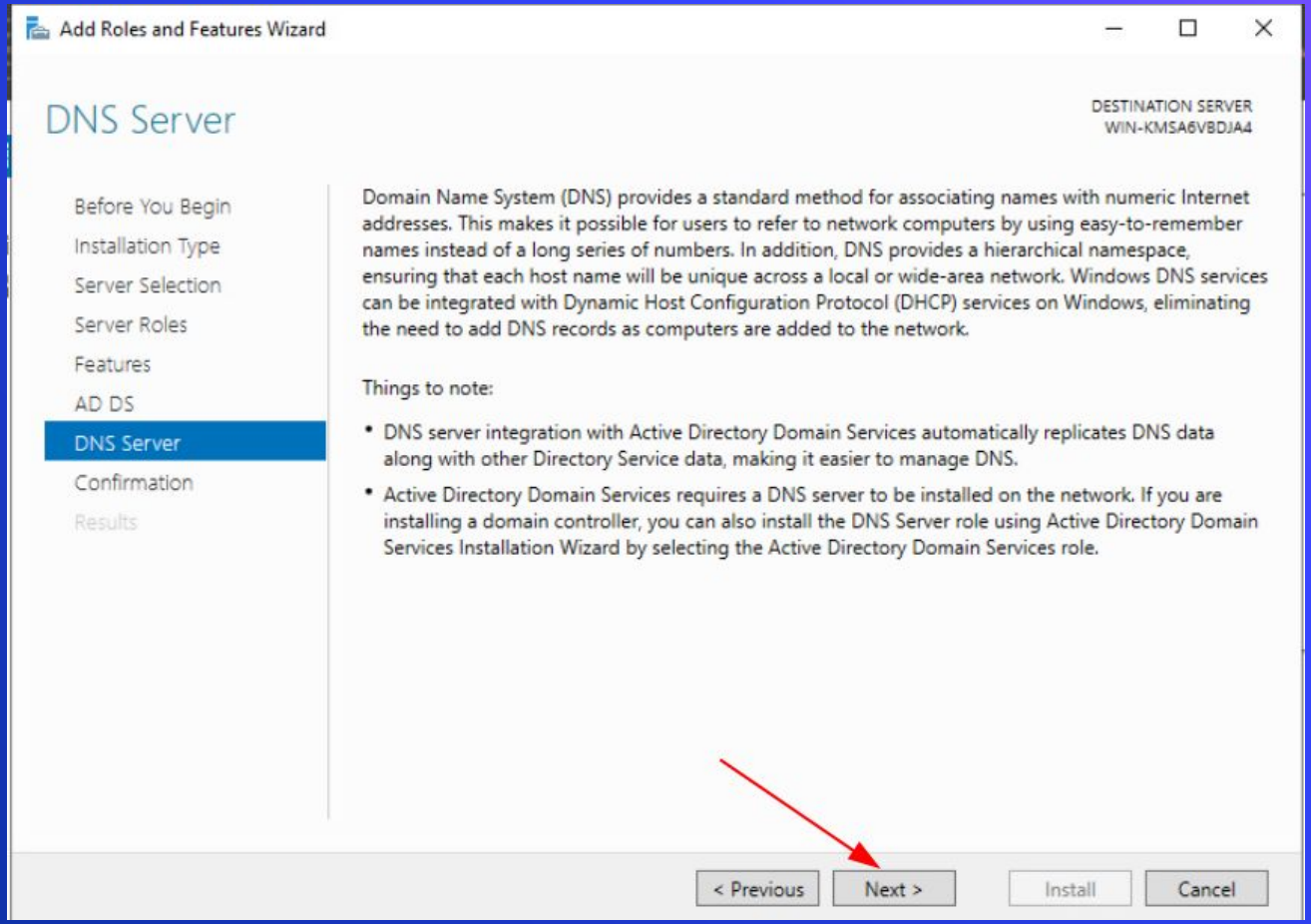

Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel

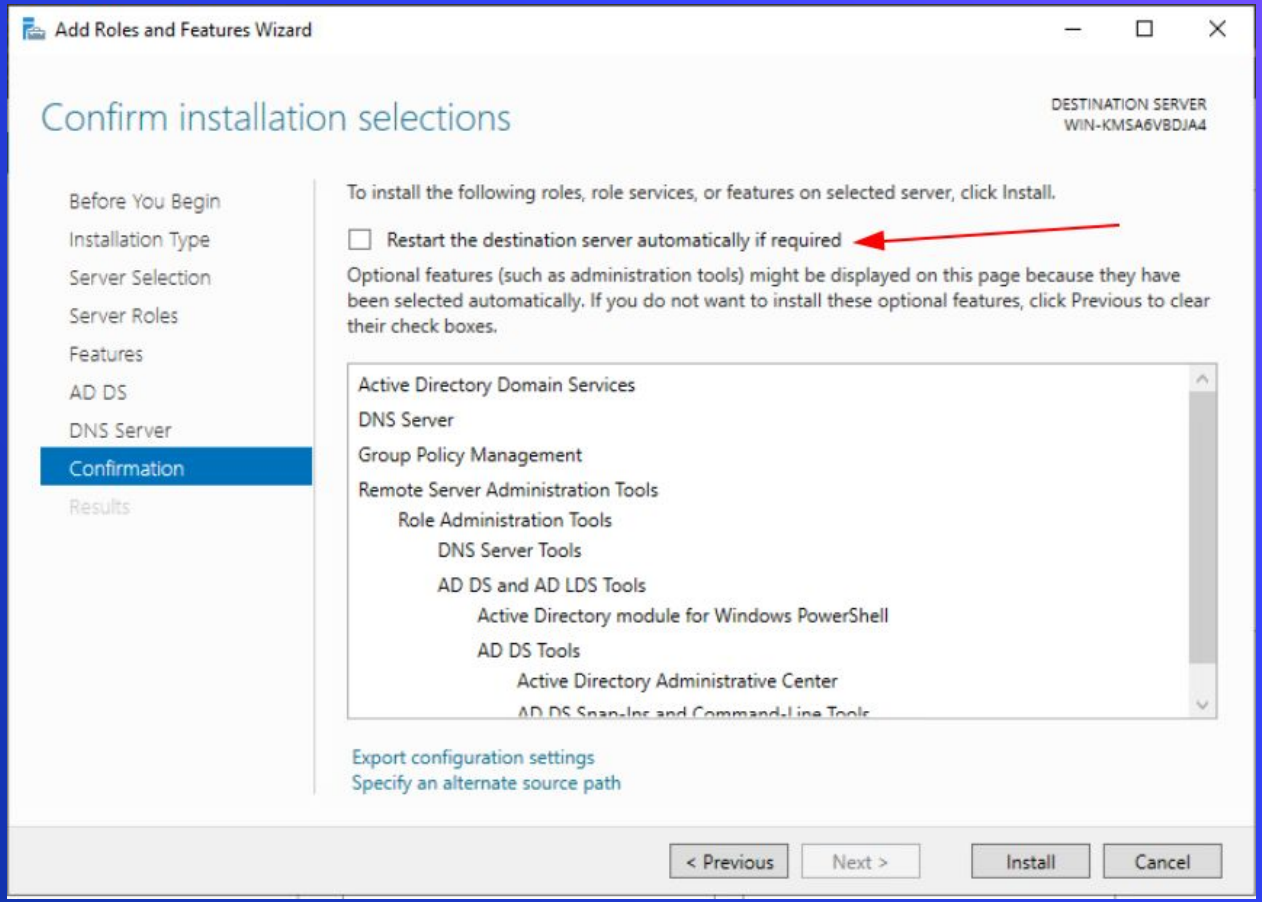

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory 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

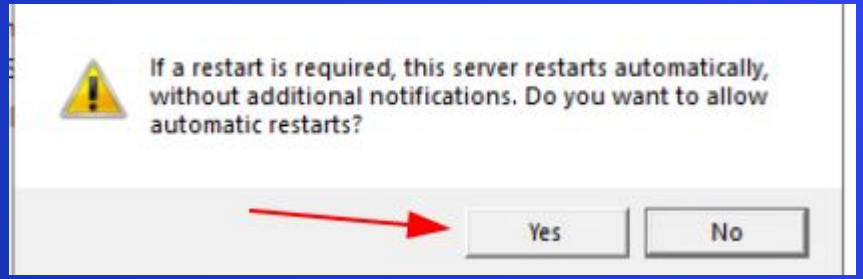

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
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

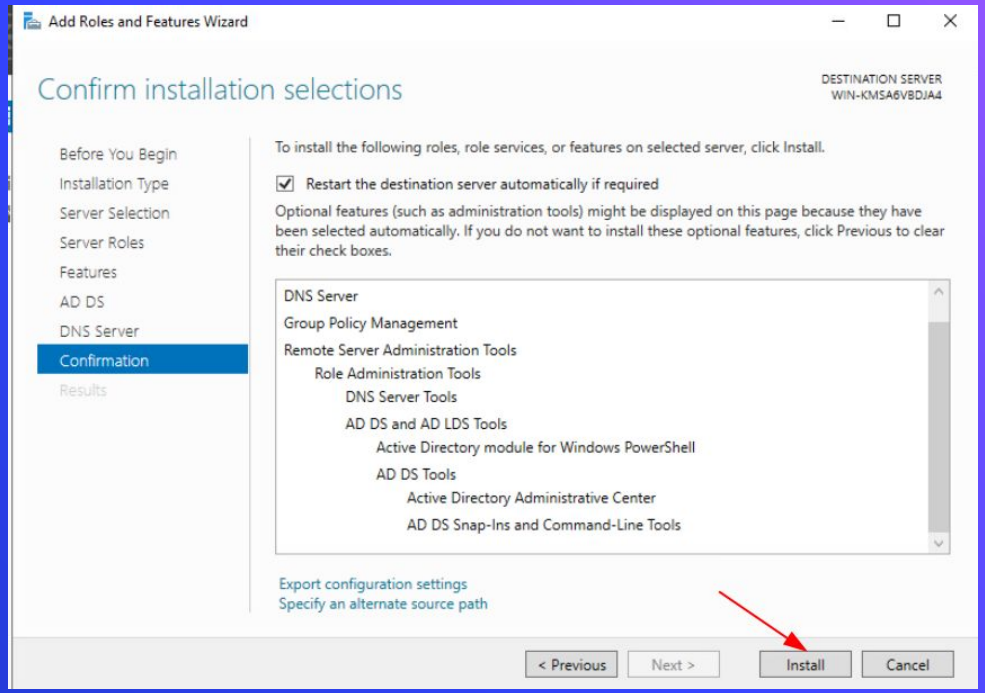

Add Roles and Features Wizard
Select features
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.7 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

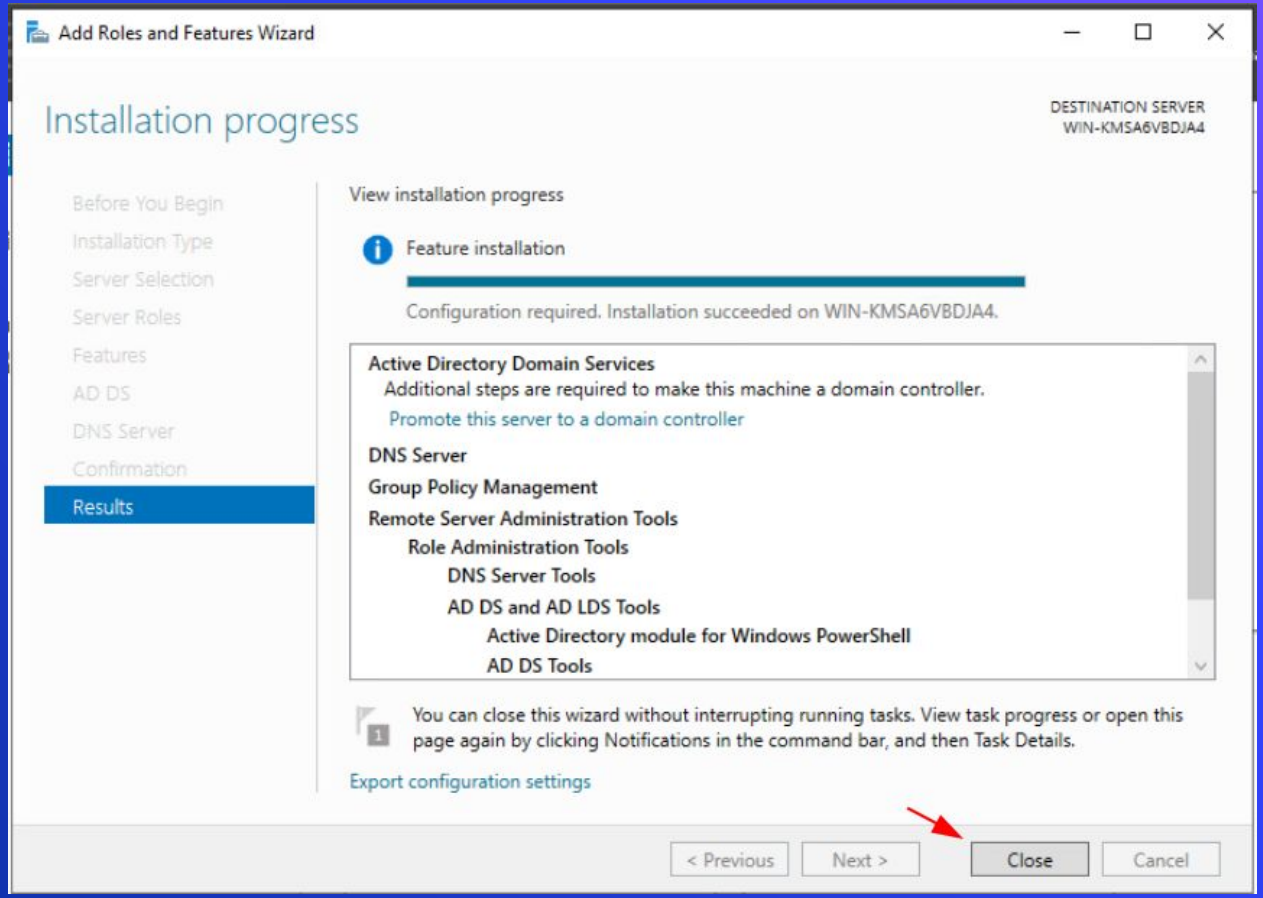

Add Roles and Features Wizard
Close
Active Directory Domain Services
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and 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

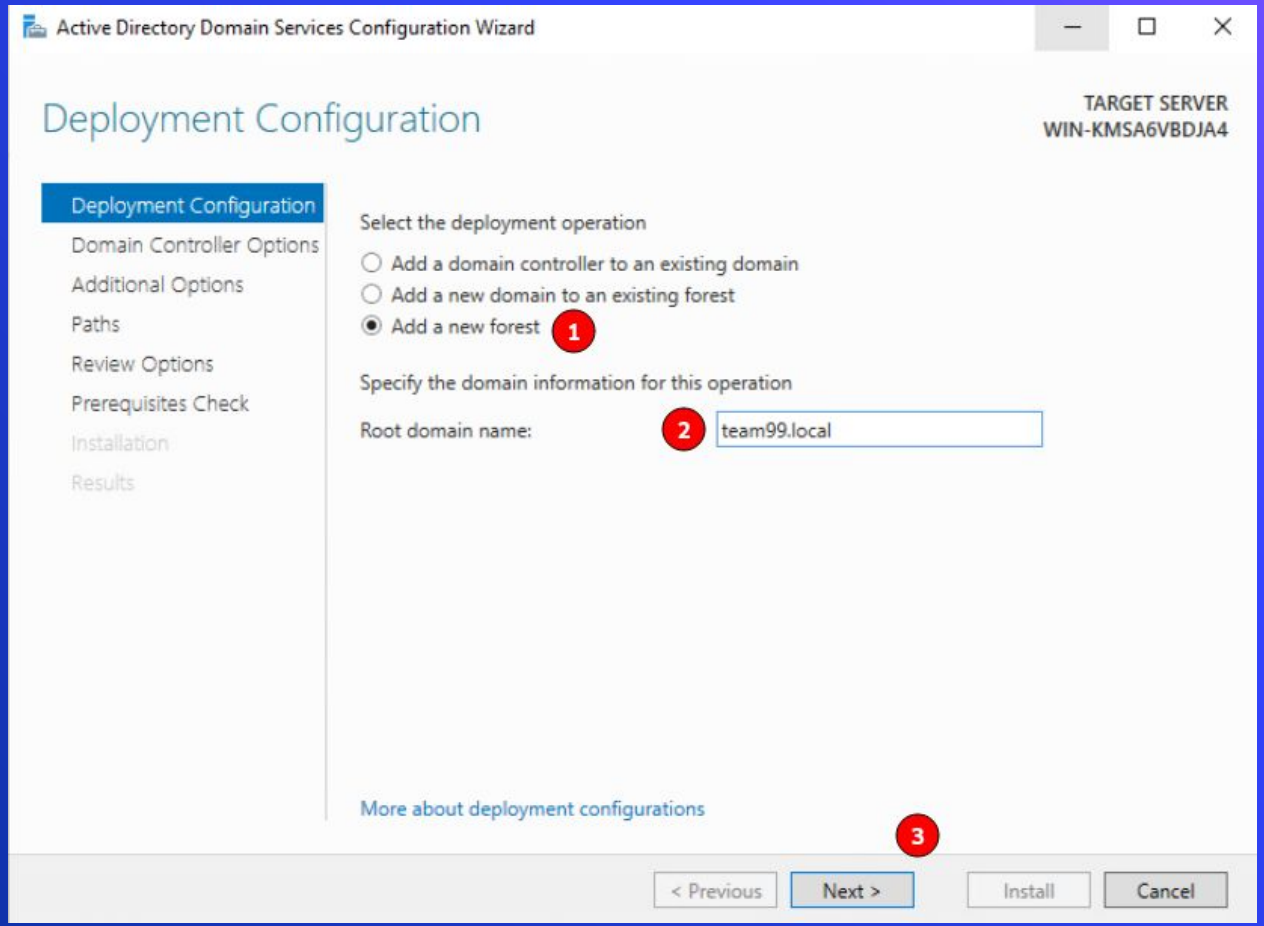

Add Roles and Features Wizard
DNS Server
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes 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

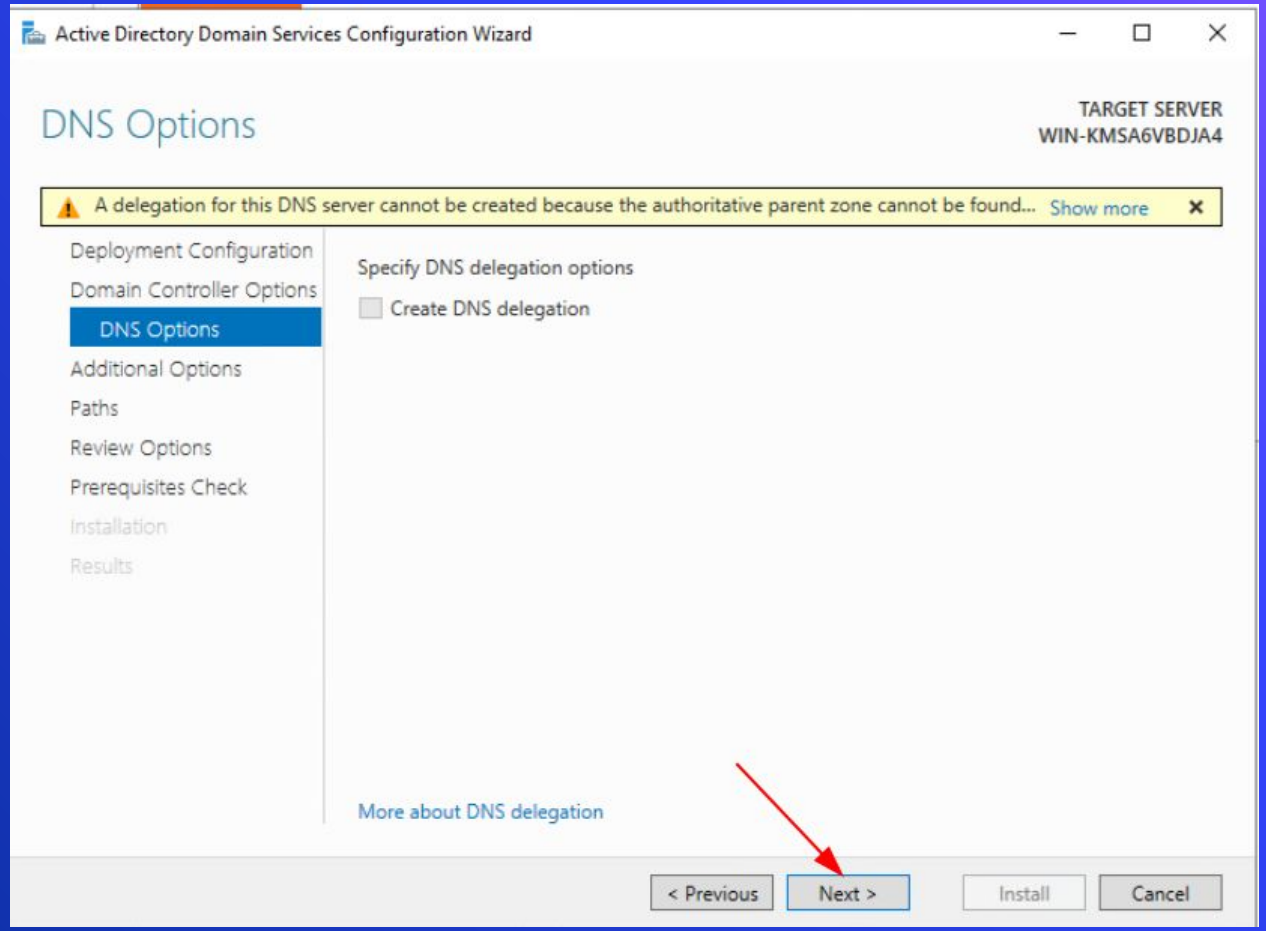

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
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
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

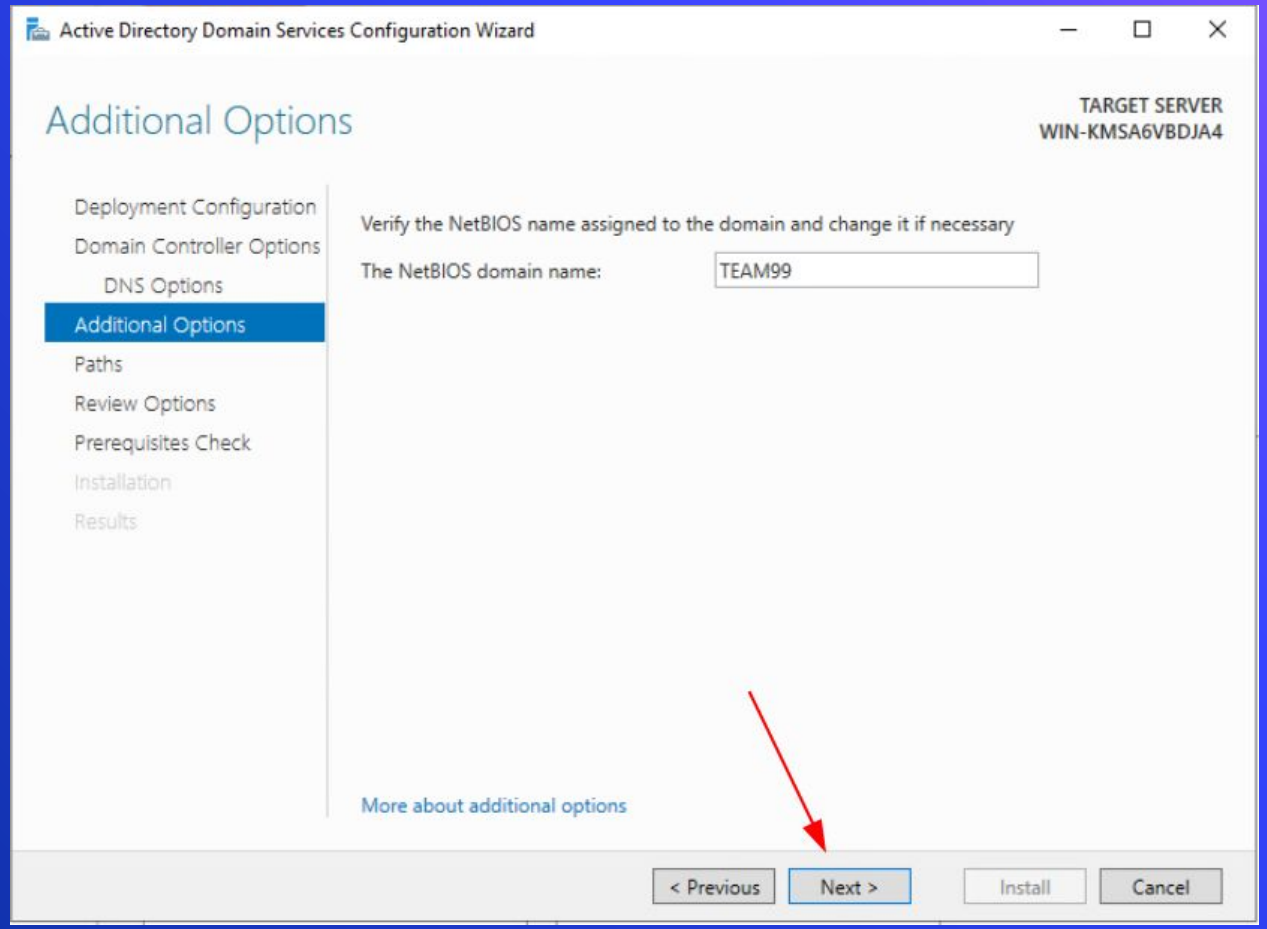

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?
Yes
No

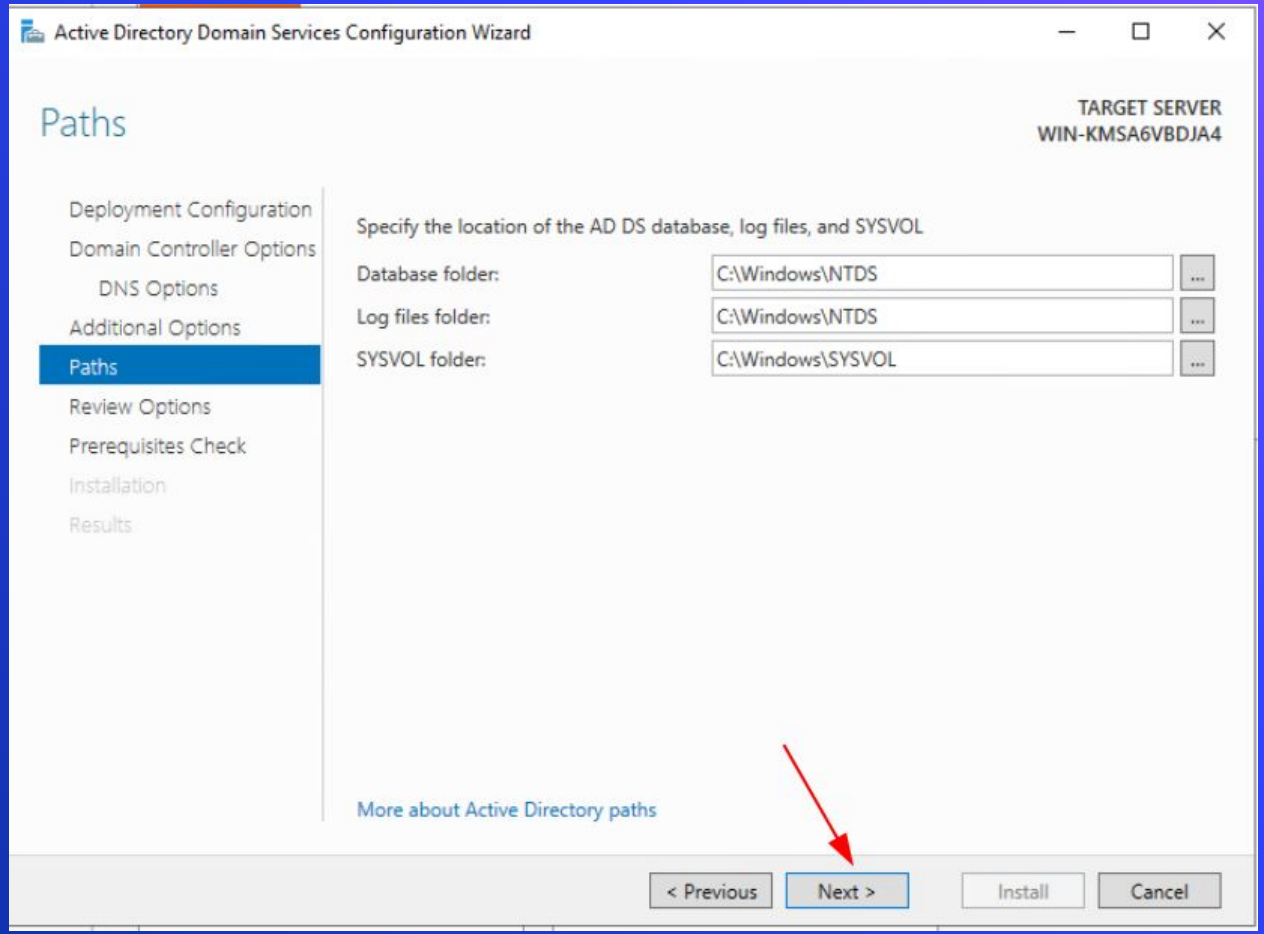

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-KMSA6V8DJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
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.
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

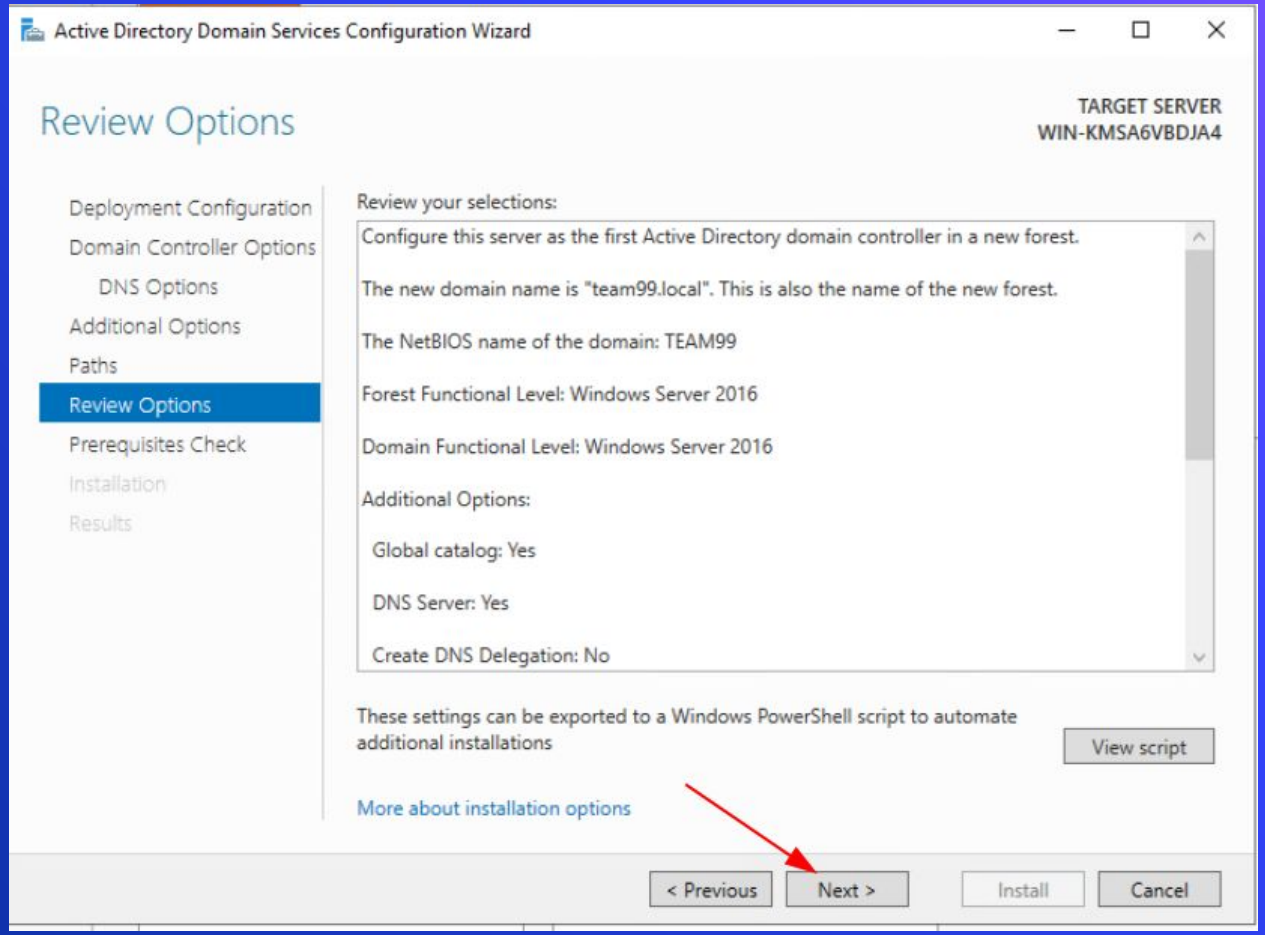

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-KMSA6VBDJA4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN-KMSA6VBDJA4.
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

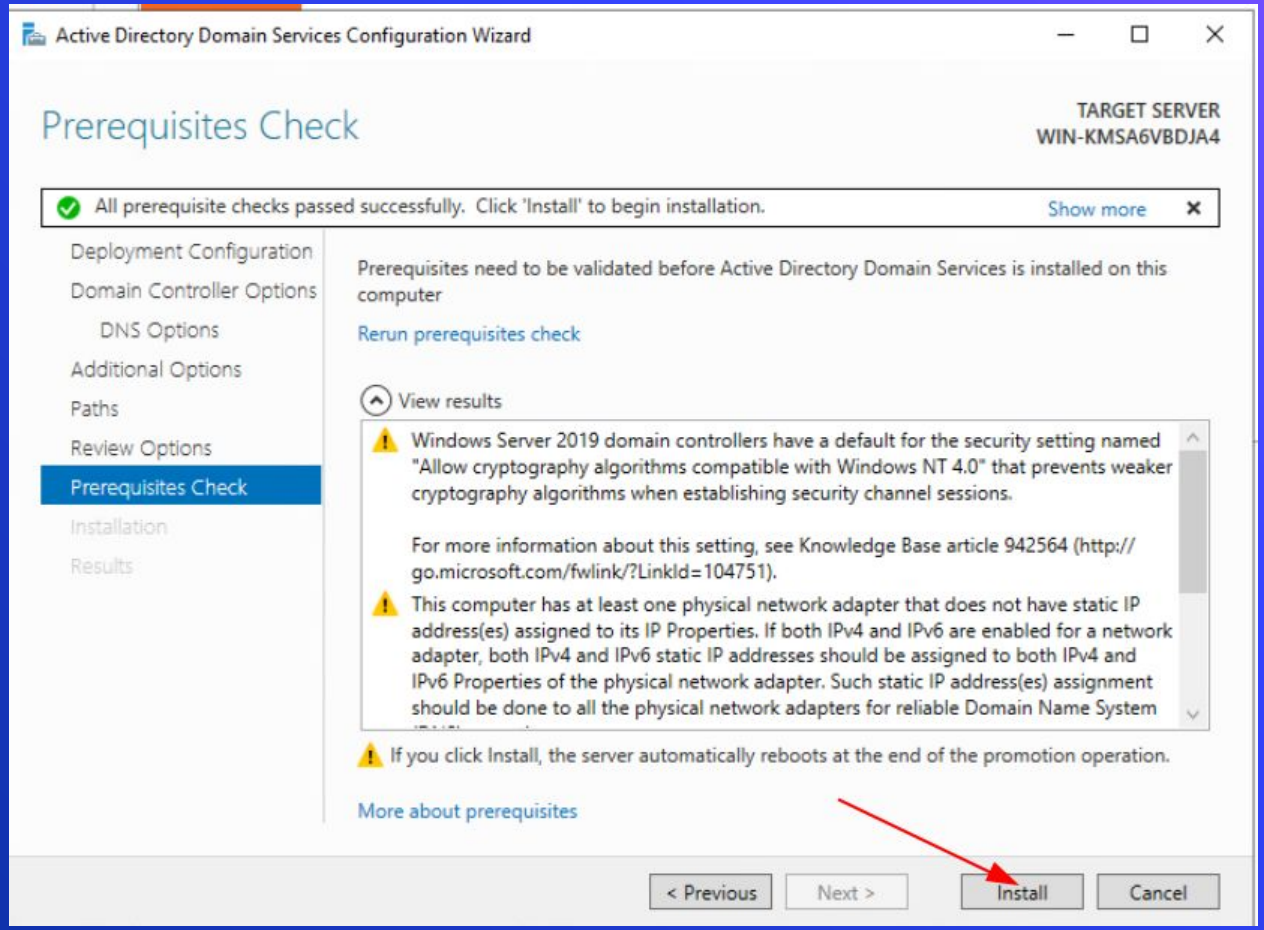

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-KMSA6VBDJA4
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an 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
team99.local
More about deployment configurations
3
< 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:
TEAM99
More about additional options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
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:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
WIN-KMSA6VBDJA4
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
Prerequisites Check
TARGET SERVER
WIN-KMSA6VBDJA4
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

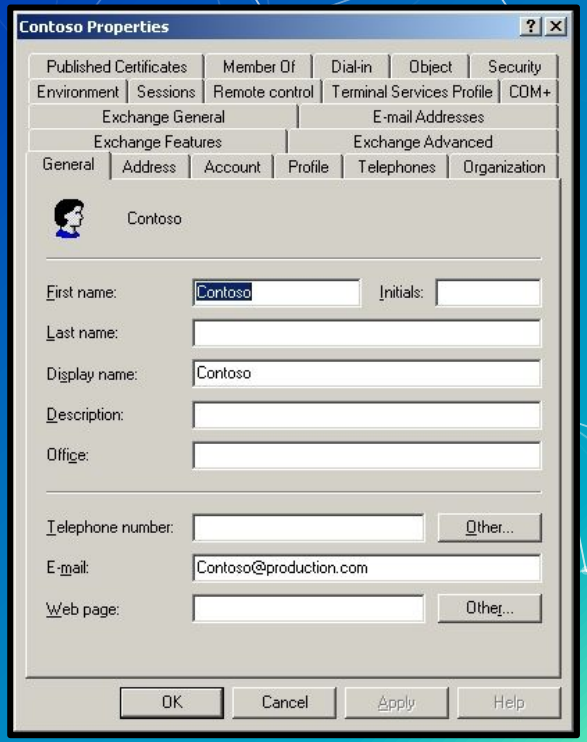
10 mins

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

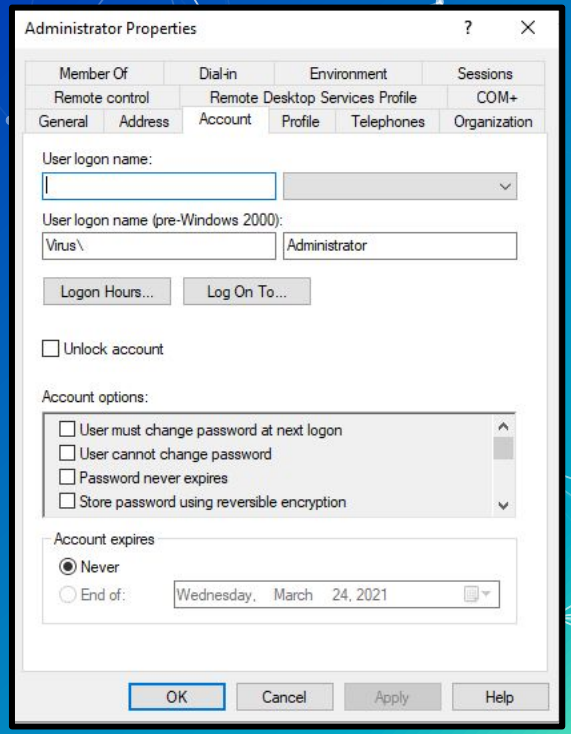
Active Directory - User Objects

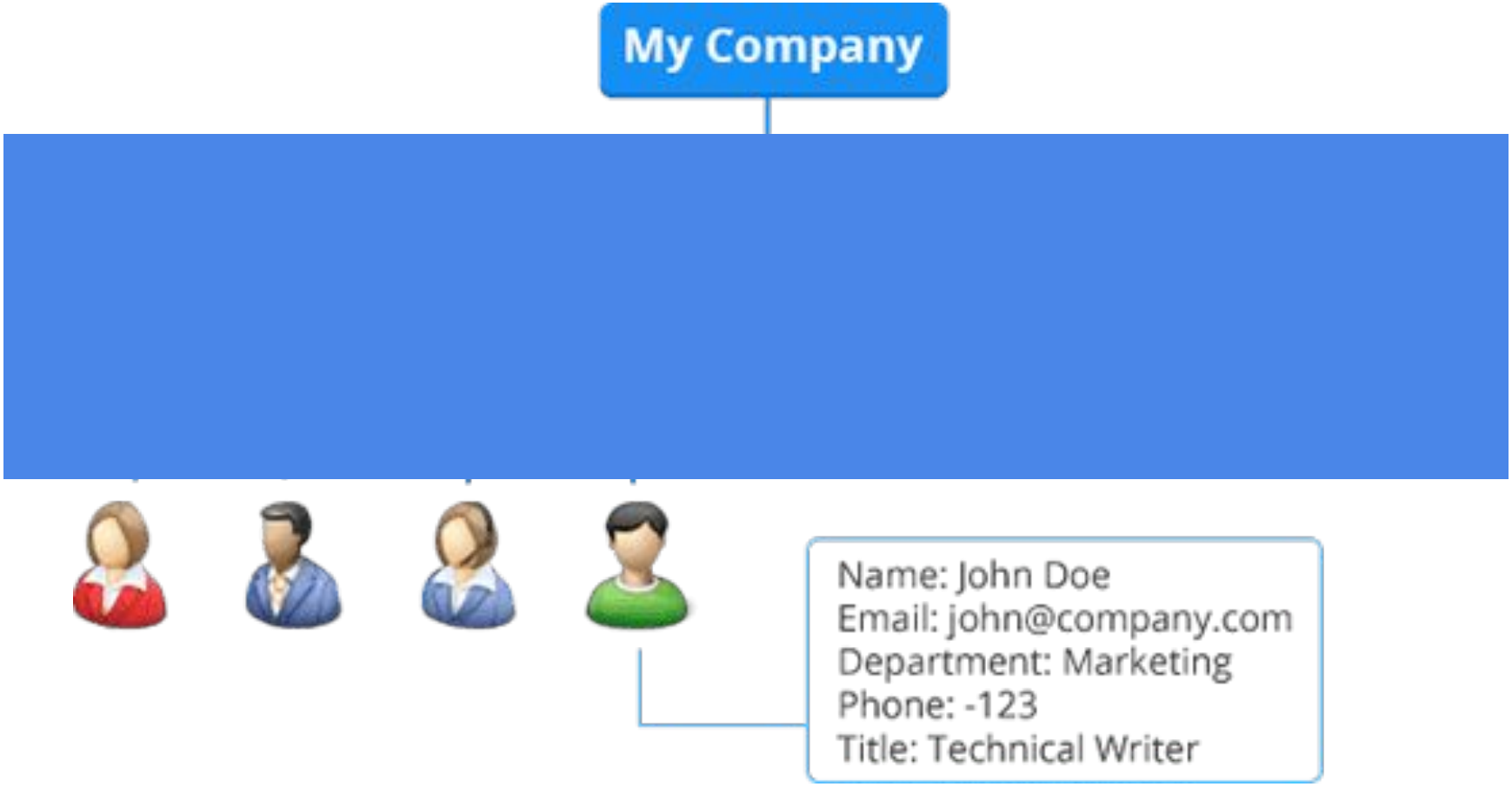
- What people authenticate against when they sign on
- Stores information on user
  - **Username**
  - Display name
  - Email
  - Phone number
  - Address
  - Location in organization
  - **Password (hashed)**



Active Directory - User Objects

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




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

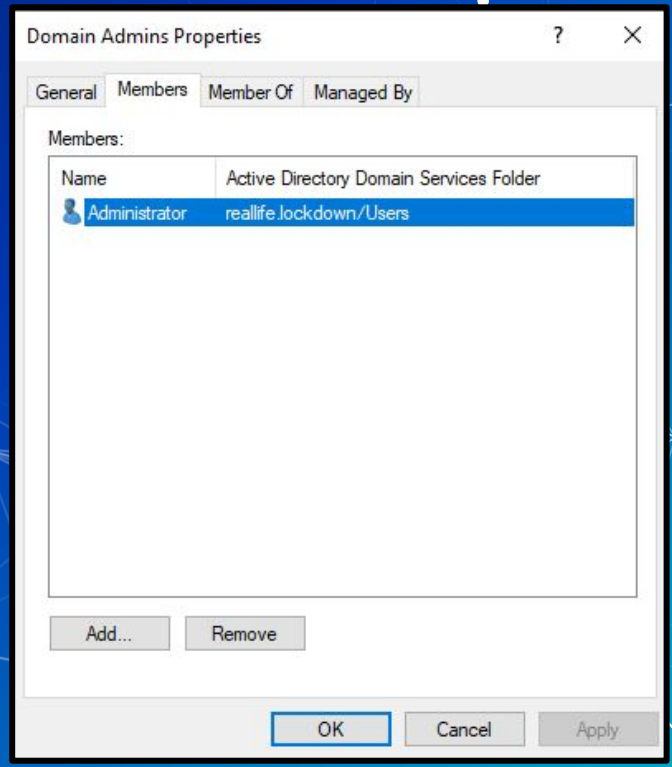
Active Directory - Security Concerns

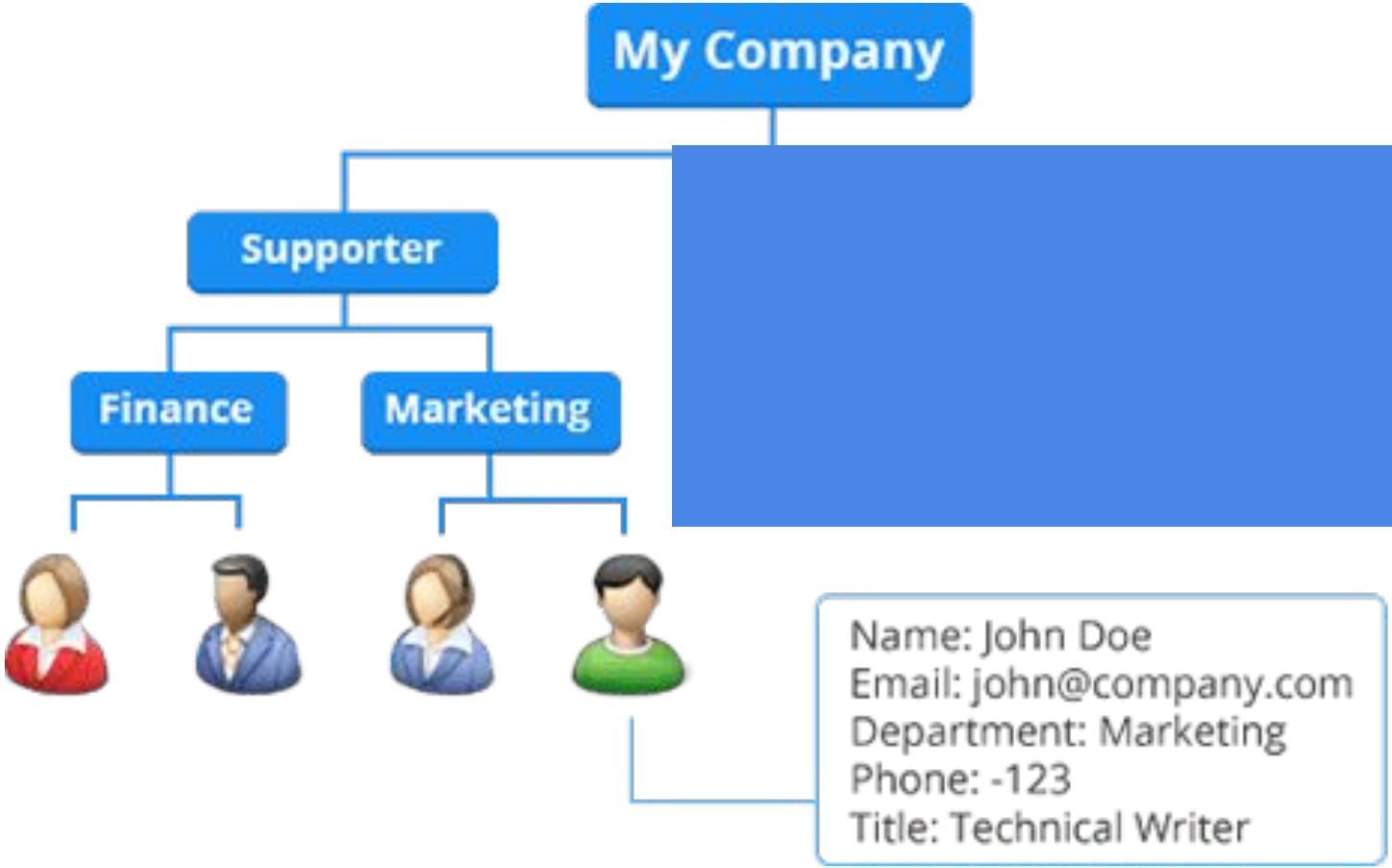
- We need a new object for each user. -> Too many to safely manage
  - UB has about 50,000 users on its main domain
- Security issues:
  - What happens when someone leaves?
  - What happens when we need to change permissions on every single student (~30K)

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 ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...




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


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

Active Directory - Nesting

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

Active Directory - Inheritance

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

Everyone can login

My Company

Only this group gets MS Office access

Parent Group

Supporter

Child Groups

Finance

Marketing

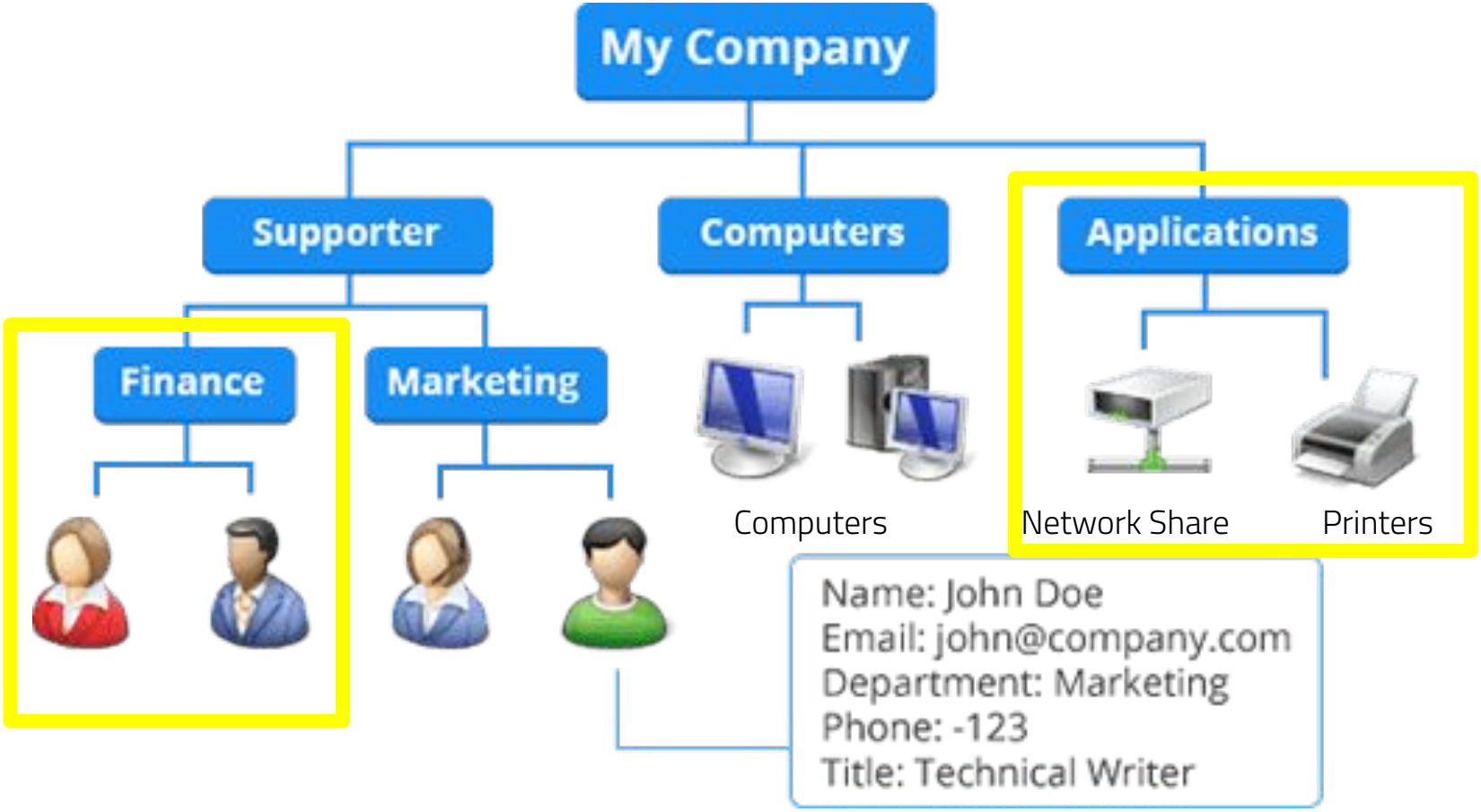
User Objects

Only marketing can use MS Paint.

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

Active Directory - Computers and Devices

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

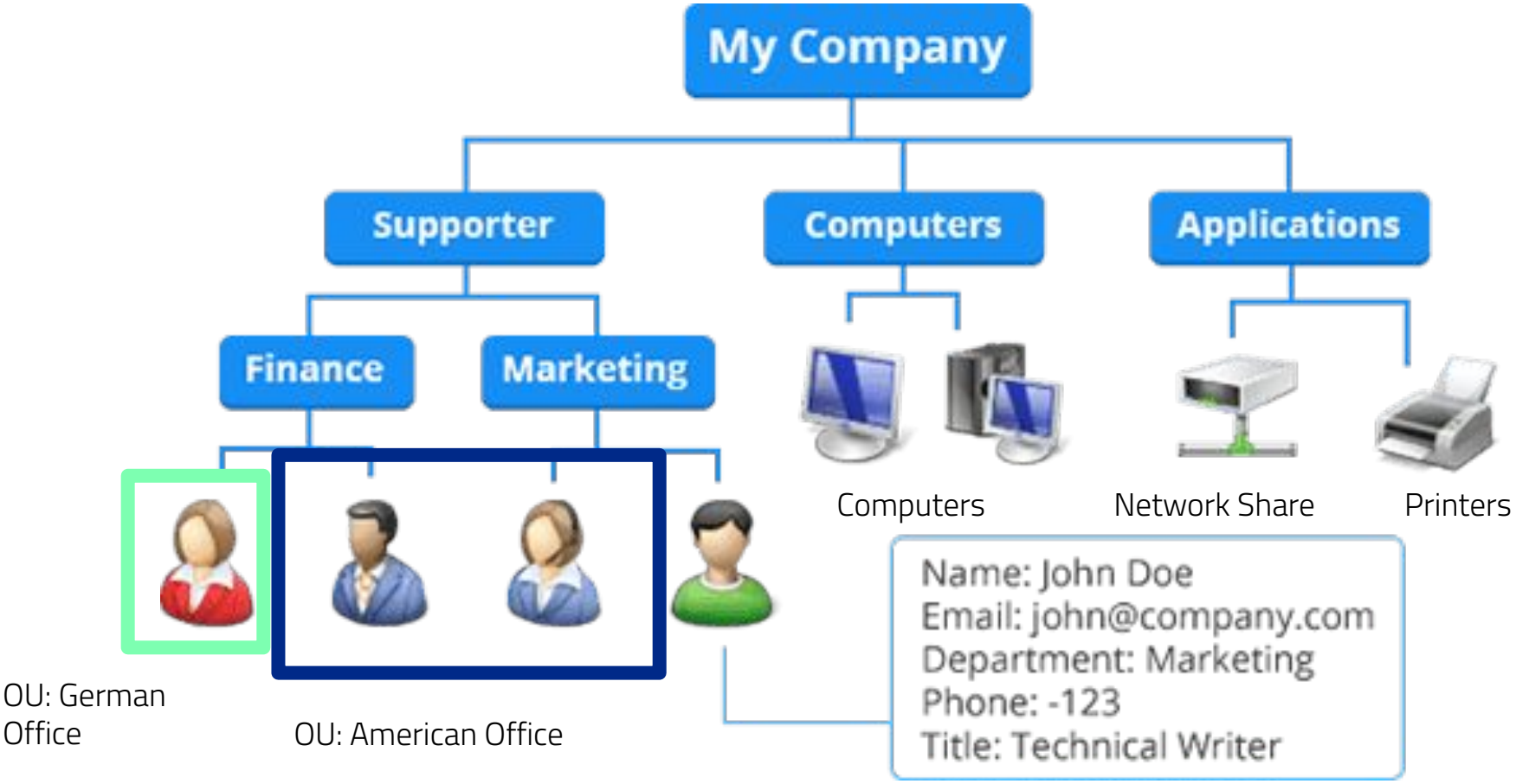

My Company
Supporter
Computers
Applications
Finance
Marketing
Computers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

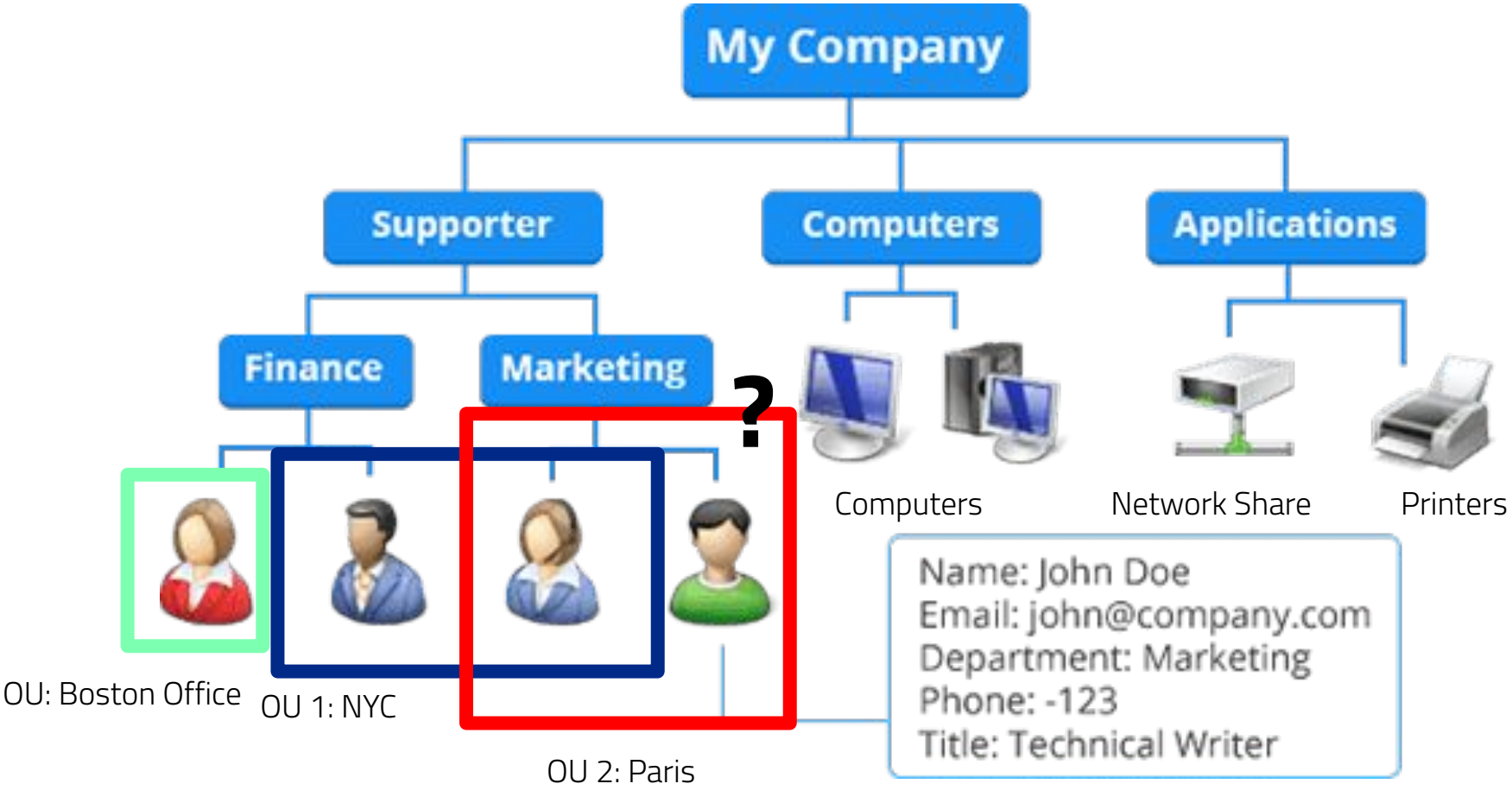
Active Directory - OUs

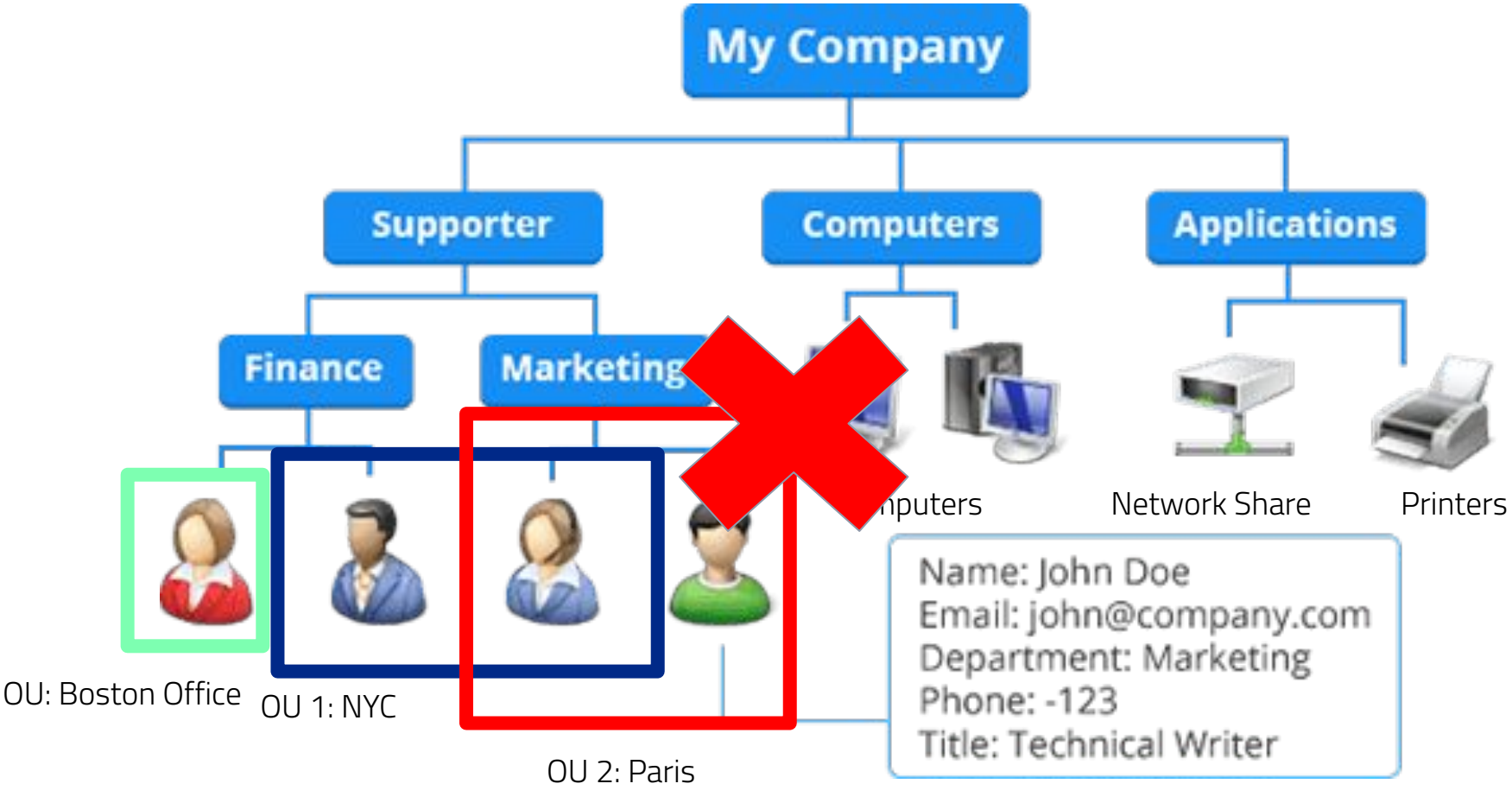
- We want the SEAS Students get a picture of Davis as their background.
- The SOM Students get a picture of Jacobs as their background.
- Are the backgrounds an IAM issue?
- How can we solve this problem?
  - What disadvantage is there to making multiple brand new security groups?

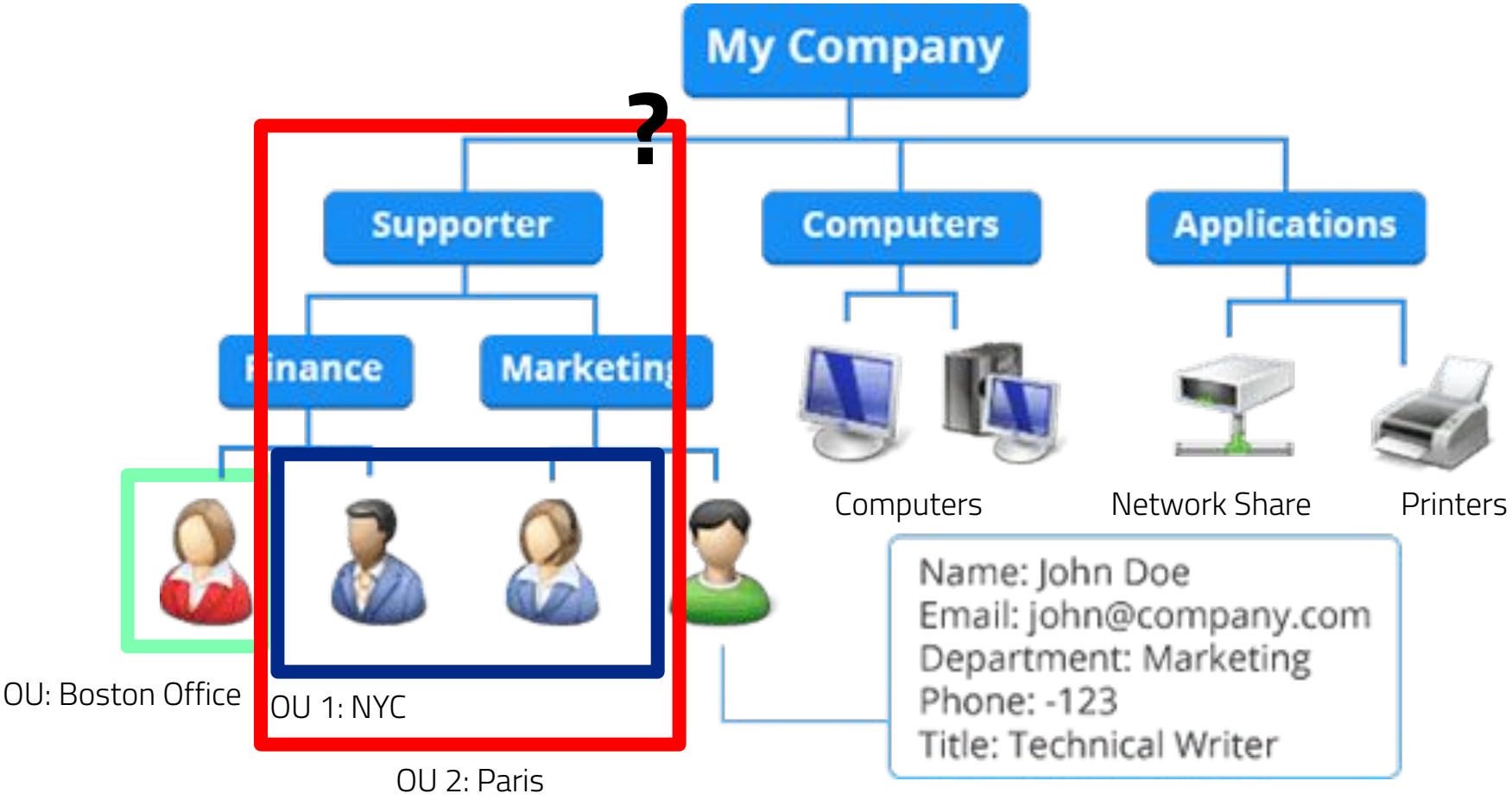
Active Directory - Organizational Units

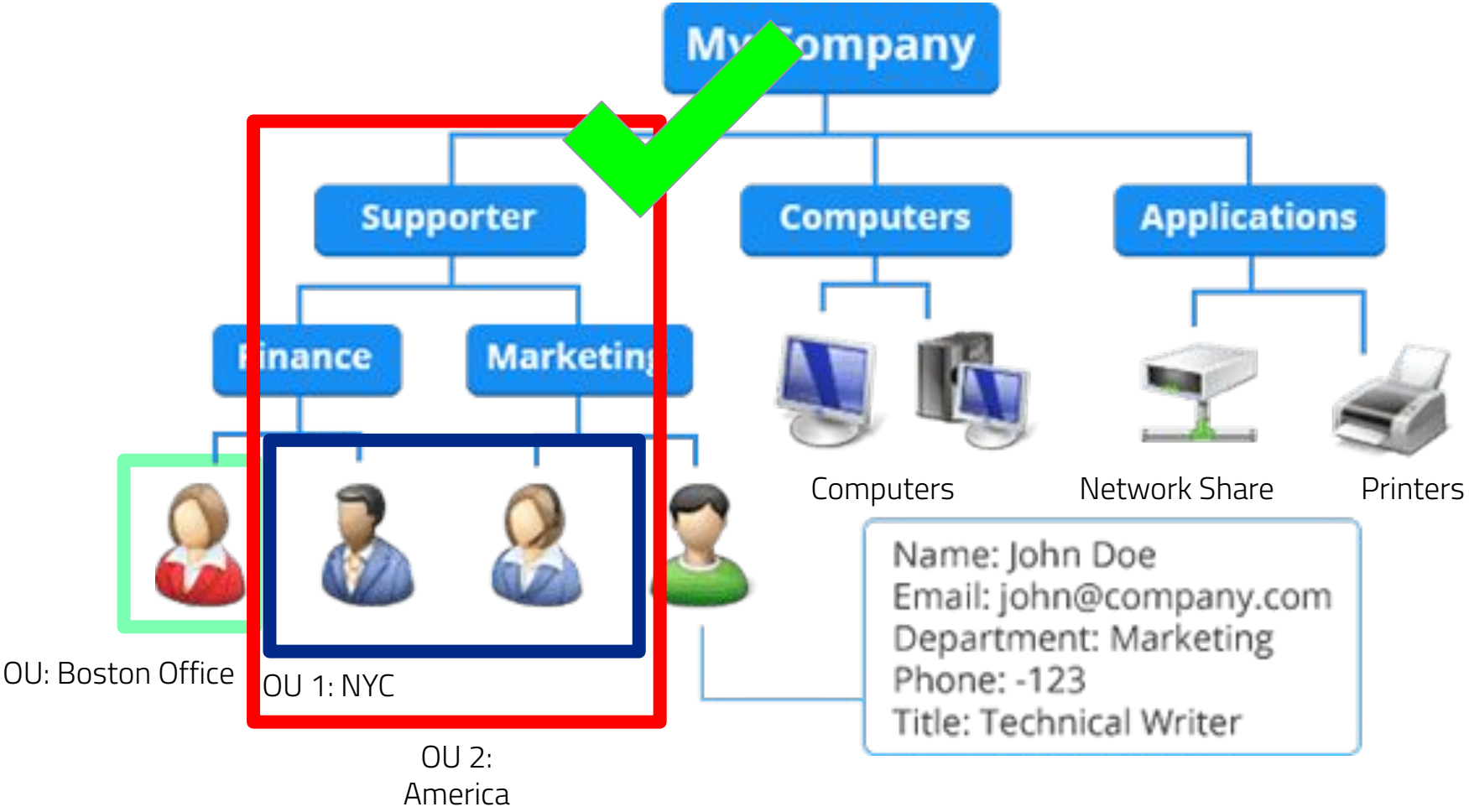
- Organizational Units (OU) are used to organize Active Directory so it's easier to manage.
- **Differ from Security Groups**
  - Security Groups are necessarily IAM based
    - ALWAYS access based
      - Student vs Faculty
  - OUs are other ways to collect objects that are not IAM based
    - Often based on location or status (like Major)
- **You can’t be in more than one OU at the same level**
- OUs cannot be security-grouped together. They are not objects. They are not groups.


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


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


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


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

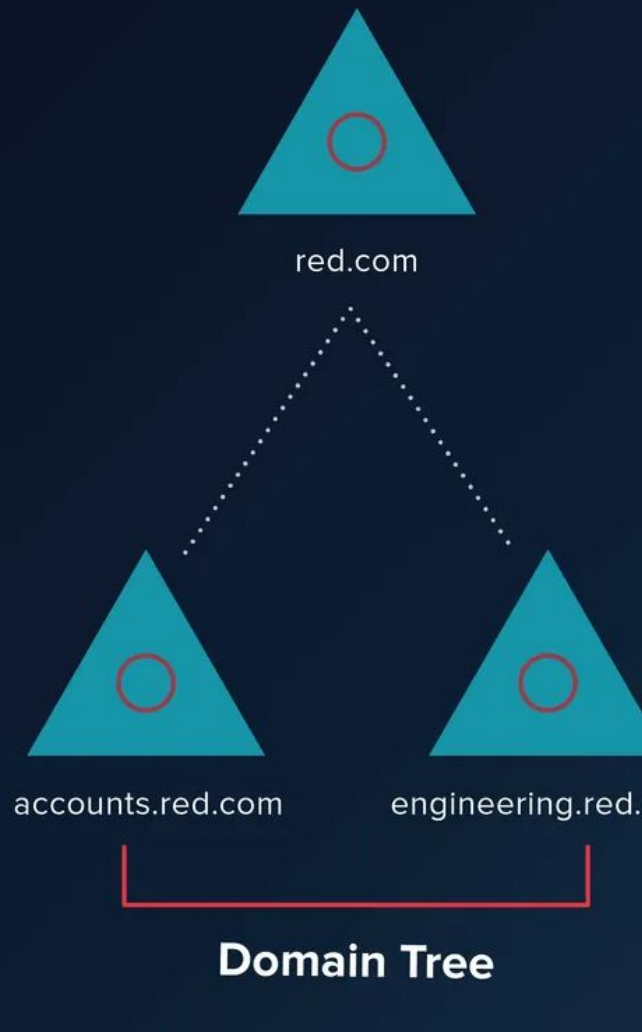

Supporter
Computers
Applications
Computers
Network Share
Printers
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer
OU: Boston Office
OU 1: NYC
OU 2:
America

Confused? TL;DR for OUs

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

Active Directory - Trees

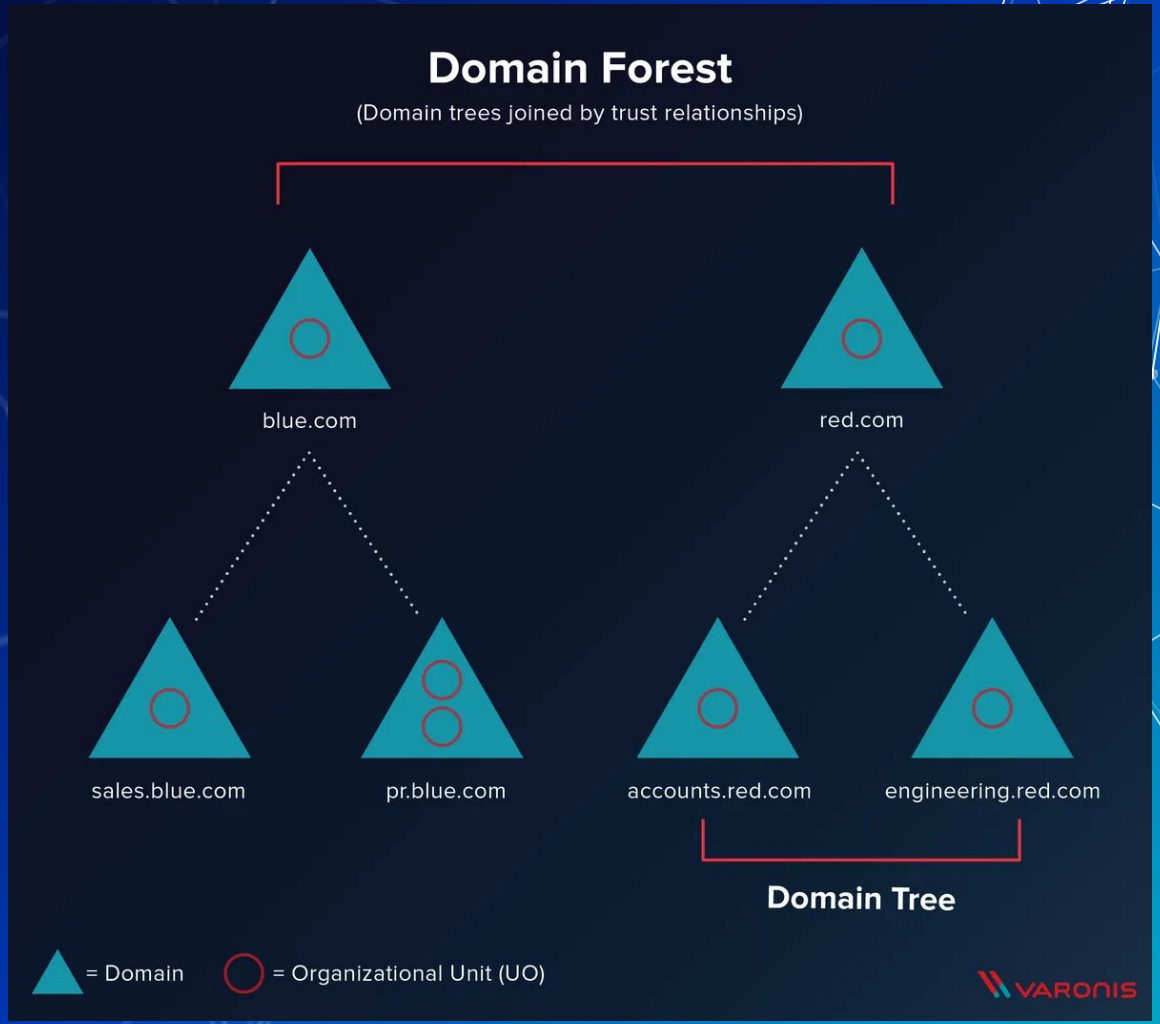
- Let's say we have a domain called red.com
  - red.com (domain) is composed of multiple objects
- red.com has 2 subdomains associated with it.
  - engineering.red.com
  - accounts.red.com
- Each subdomain can be used to further **organize** the objects associated with company.xyz
- These subdomains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



Active Directory - Forests

- Let's say that Red Company buys Blue Company
  - Blue is now a subsidiary of Red.
- Company Red already has a domain set up. Red can now manage the domains of Red and Blue together.

- Multiple Trees can be managed together
  - This hierarchy is called an AD **Forest**.
- A forest is a collection of one or more domain trees.
- As soon as you make a domain, you also have a tree (of 1 domain) and a forest of 1 tree


Domain Forest
(Domain trees joined by trust relationships)
blue.com
red.com
sales.blue.com
pr.blue.com
accounts.red.com
engineering.red.com
Domain Tree
= Domain
= Organizational Unit (UO)
VARONIS

QUESTIONS?

Break

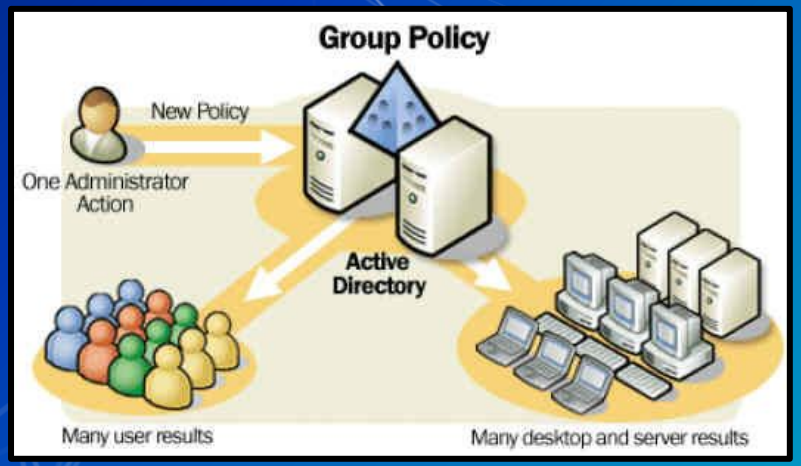
Please return in 10 mins

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

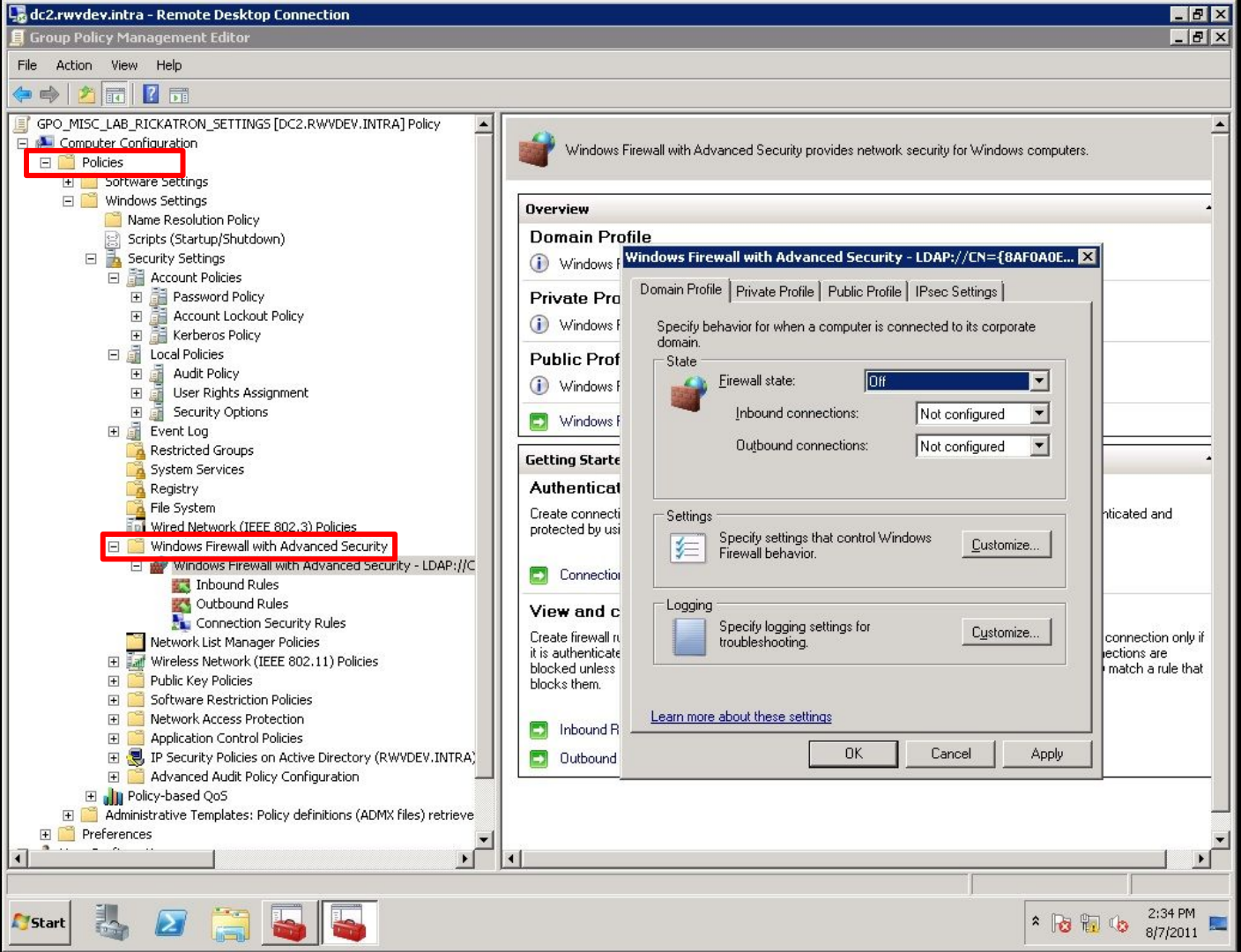


Group Policy Examples

- 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

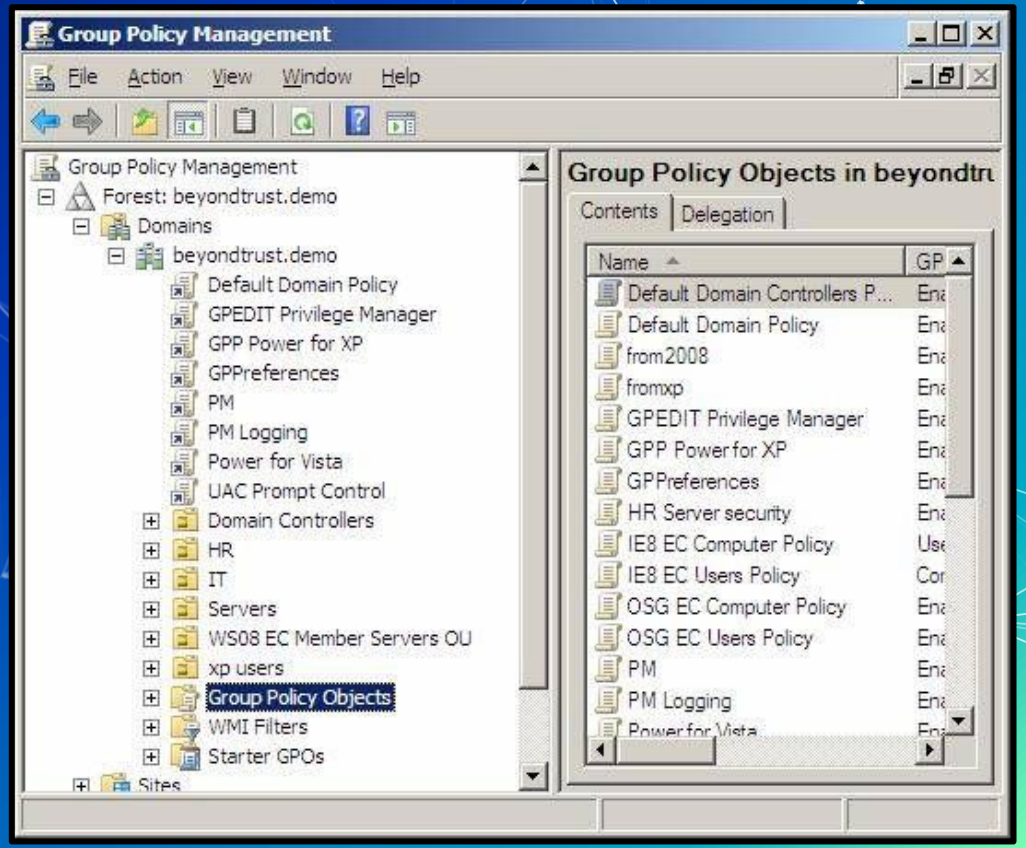
Group Policy Key Terms

- 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


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
Private Pro
Public Prof
Getting Starte
Authenticat
View and c
Windows Firewall with Advanced Security - LDAP://CN={8AF0A0E...
Domain Profile
Private Profile
Public Profile
IPsec Settings
Specify behavior for when a computer is connected to its corporate domain.
State
Firewall state:
Off
Inbound connections:
Not configured
Outbound connections:
Not configured
Settings
Specify settings that control Windows Firewall behavior.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
Learn more about these settings
OK
Cancel
Apply
Start
2:34 PM
8/7/2011

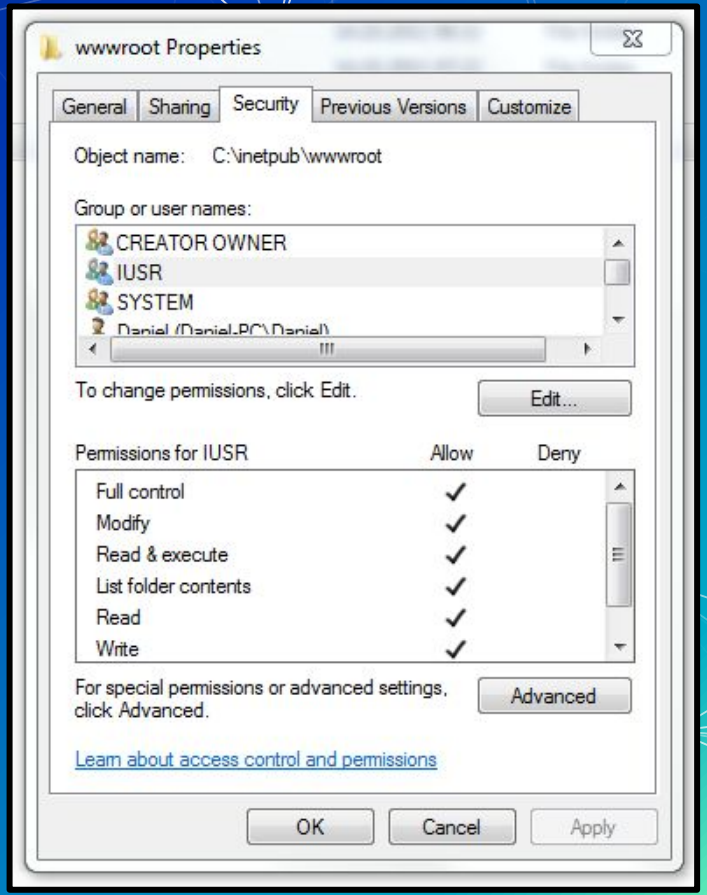
Multiple Group Policies

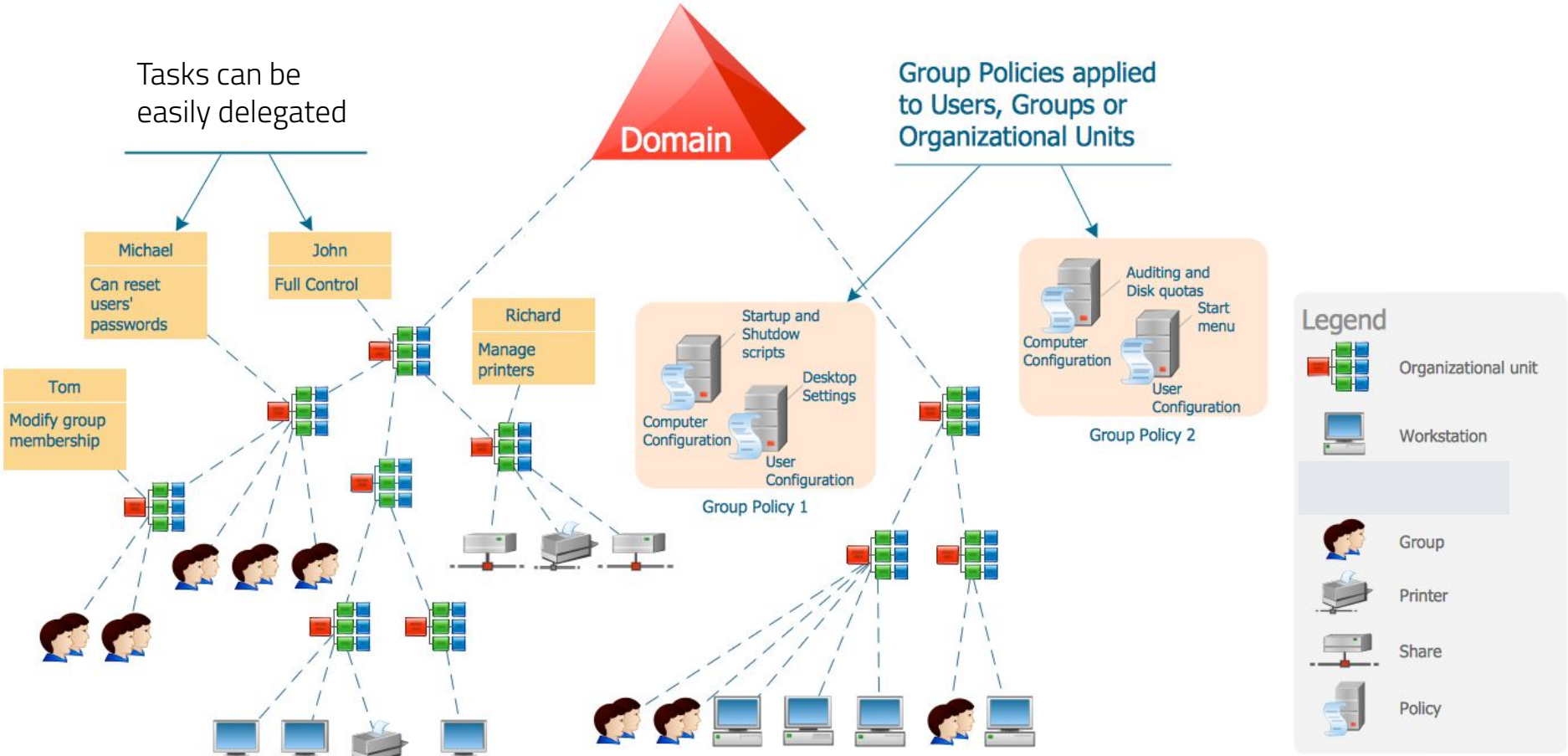
- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group
- **Group policies can be applied to any domain object**
  - Users, Computers, Groups, OUs



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

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

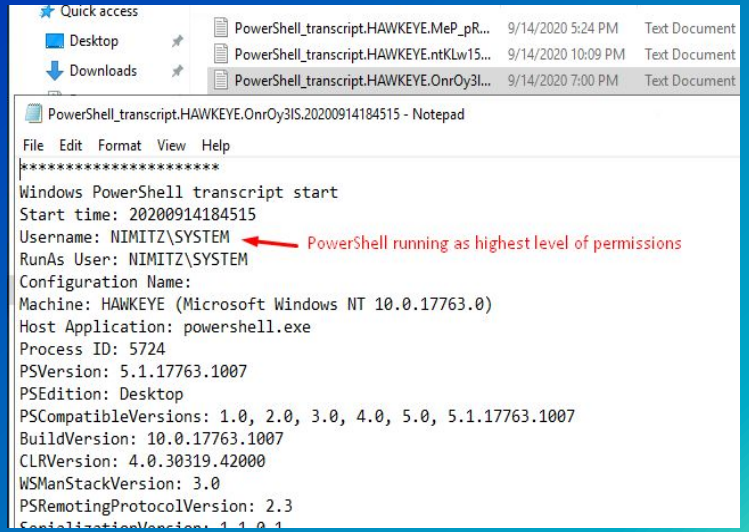
PowerShell Execution Policies

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

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

PowerShell Transcription

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




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

Windows protects Defender's registry keys

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