Windows Server 2016

Server OS

- A server operating system, is specifically designed to run on servers, which are specialized computers that operate within a client/server architecture to serve the requests of client computers on the network.
- The latest windows Server OS is **Windows Server 2022**

- Windows Server is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications management.
- Windows Server have focused on stability, security, networking, and to offer a centralized administration to enterprise companies.
- A Client will request for service and server will offer services to other systems

Some of the server services

- Web service
- Email service
- DNS service
- DHCP service
- File service
- Application service
- Print service
- Database service
- VPN service etc…

Windows Server 2016 Capabilities

Edition	Ideal for...	Visualization rights	Licensing model	Client Access Licenses	RAM Limit	CPU Limit
Essentials	Small businesses with basic IT requirements; very small or no IT department	no, one physical **or** one virtual installation	CPU-based	CALs not required * (limited to 25 users / 50 devices)	64 GB RAM	max. 2 CPUs
Standard	For all companies that require advanced features and virtualize to a lesser extent	2 virtual machines ** **or** 2 Hyper-V Container	Core-based	CALs required ***	24 TB RAM	512 Cores
Datacenter	For all companies with high requirements on IT workloads with large number of virtual systems	unlimited virtual machines and Hyper-V Container				

Windows Server Editions
Windows Server 2016
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2
Windows Server 2008
Windows Server 2003 R2
Windows Server 2003
Windows Server 2000
Windows NT 4.0
Windows NT 3.51

Windows Server 2016

Edition	Purpose
Windows Server 2016 Essentials	Designed for small businesses
Windows Server 2016 Standard Edition	Designed for physical server environments with little to no virtualization
Windows Server 2016 Datacenter Edition	Designed for highly virtualized environments – including cloud and hybrid cloud environments
Microsoft Hyper-V Server 2016	Acts as a stand-alone virtualization server for virtual machines
Windows Storage Server 2016 – Workgroup Edition	Allows 50 users, one processor core, and 32 GB of RAM. Supports domain joining
Windows Storage Server 2016 – Standard Edition	Supports up to 64 sockets but is licensed on a two-socket, incrementing basis

Windows Server 2016 Installation Requirements

Hardware Requirements

Component	Requirement
Processor architecture	64-bit
Processor speed	1.4 gigahertz (GHz)
RAM	512 MB / 2GB
Hard drive space	32 GB

Note: VM Setup will fail if only 512 MB:

To resolve:

(1) Allocate > 800 MB RAM or

(2a) Use Diskpart.exe create a partition

(2b) Run createpagefile command

Additional Recommendations

- UEFI 2.3.1c for Secure Boot

Windows 2016 Features

- PowerShell 5.0
- PowerShell is the new Command Prompt. More than that, PowerShell is arguably the most powerful configuration tool for every aspect within Windows Server.
- In fact, some features in Windows cannot even be performed without PowerShell; it is becoming that integral.
- Windows Server 2016 will see a significant number of new PowerShell cmdlets focused on specific functionality.

Windows Defender

- Built-in malware protection
- Microsoft has been including its own malware protection in the client operating systems since Windows 8, but never before on a server platform.
- Windows Defender has been improved, and it now runs by default in Windows Server 2016

- Soft restart
- In an effort to speed up reboots, there is an optional reboot setting now called soft restart.
- So what is a soft restart? It is a restart without hardware initialization. In other words, it restarts the operating system without restarting the whole machine.

Soft Start

- Using the shutdown command:
- shutdown /r /soft /t 0 /r = restart
- Using the Restart-Computer cmdlet:
- Restart-Computer -Soft

- Nano Server
- Unfortunately, the previous version's Server Core is going largely unused, but Microsoft expects this to change completely with the release of Nano Server in Windows Server 2016.

- Nano Server has a greatly decreased security footprint, and incredibly small hardware requirements.

- In the next few years, it is expected that many companies will swing a lot of their workloads from traditional servers over to Nano Servers.

- Nano is the end result of Microsoft refactoring the core pieces of Windows Server to its minimally functional state.
- It's so minimal, in fact, that it doesn't have any direct user interface besides the new Emergency Management console.
- A Nano instance is managed remotely using Windows PowerShell, or other tools, to include the process of adding new roles.

Storage Replica

- Microsoft has supported replication in the world of Hyper-V, but it has been limited up to this point to asynchronous replication of virtual hard disks.
- That changes with Windows Server 2016, as you now have the ability to replicate entire volumes at the block level.
- Further, you can choose between synchronous and asynchronous replication.

Hyper-V hot add NICs and memory

- Previous versions of Hyper-V did not allow you to add a network interface or more memory to a running virtual machine.
- Downtime is always bad but change is sometimes good.
- Microsoft now allows you to make some critical machine configuration changes without taking the virtual machine offline. The two most important changes involve networking and memory.

Nested Virtualization

- Nested virtualization refers to the capability of a virtual machine to itself host virtual machines.
- This has historically been a "no go" in Windows Server Hyper-V, but we finally have that ability in Windows Server 2016.
- Nested virtualization makes sense when a business wants to deploy additional Hyper-V hosts and needs to minimize hardware costs.

Secure Boot

- Secure Boot is part of the Unified Extensible Firmware Interface (UEFI) specification that protects a server's startup environment against the injection of rootkits or other assorted boot-time malware.
- **ReFS**
- The Resilient File System (ReFS) has been a long time coming in Windows Server. In Windows Server 2016, we finally get a stable version. ReFS is intended as a high-performance, high-resiliency file system intended for use with Storage Spaces Direct and Hyper-V workloads.

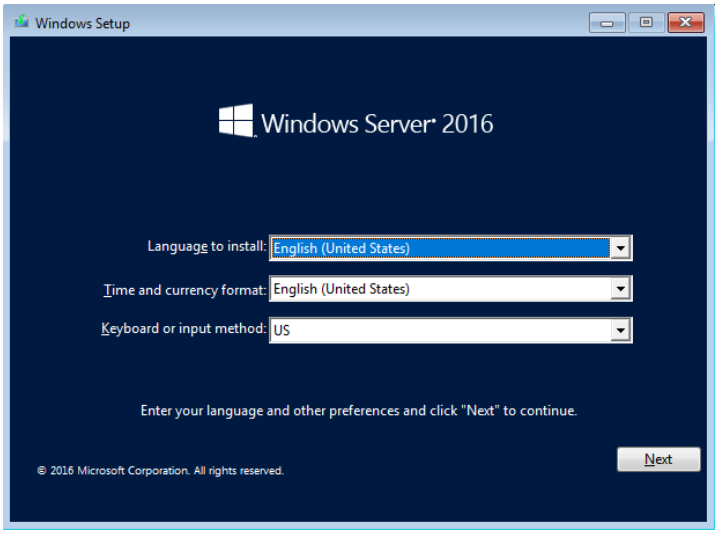
- Web Application Proxy
- Web Application Proxy (WAP) is a role that was introduced in Windows Server 2012 R2 and provides us with the ability to reverse proxy web applications.
- Number of new functions have been provided with the Server 2016 version, on remote access technology.

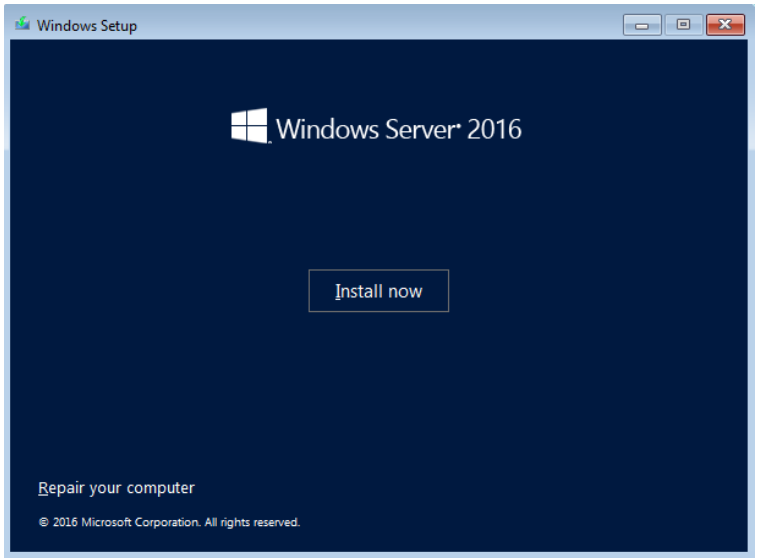
- Shielded virtual machines
- So many companies are running a majority of their servers as virtual machines today. One of the big problems with this is that there are some inherent security loopholes that exist in the virtualization host platforms of today.

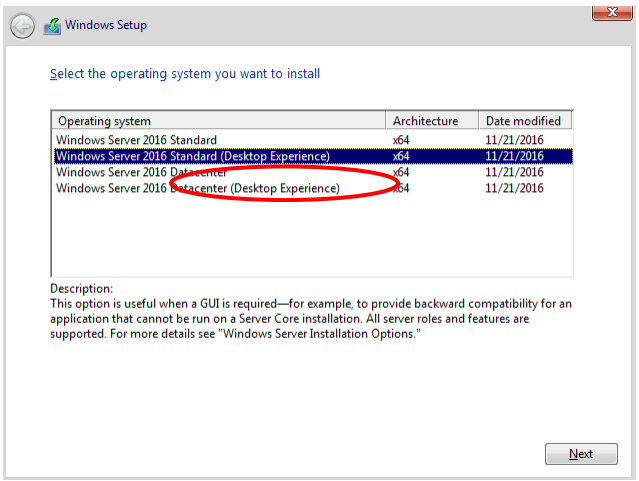
- One of those holes is backdoor access to the hard disk files of your virtual machines.

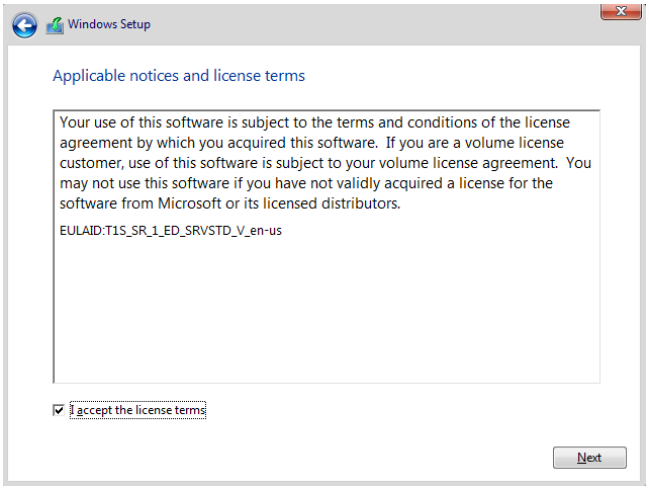
- It is quite easy for anyone with administrative rights on the virtual host to be able to see, modify, or break any virtual machine that is running within that host.

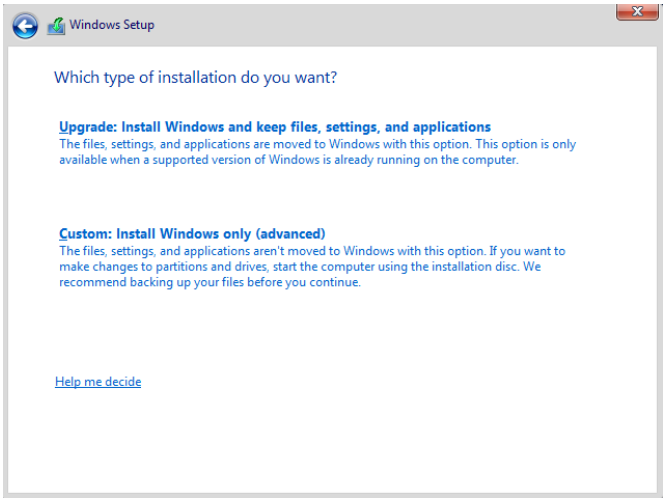
Windows Server 2016 Installation

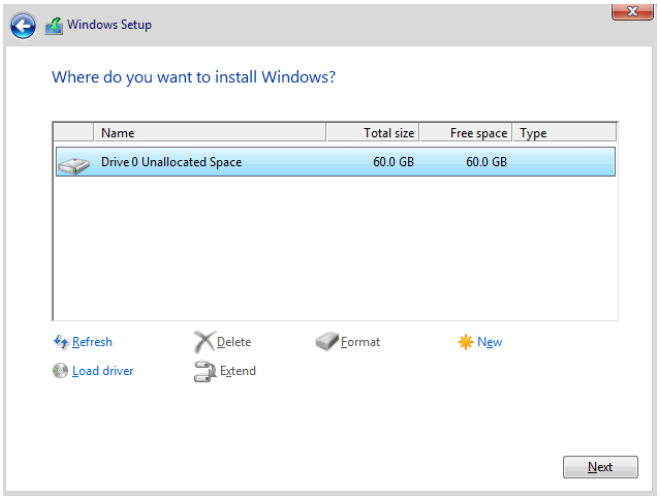


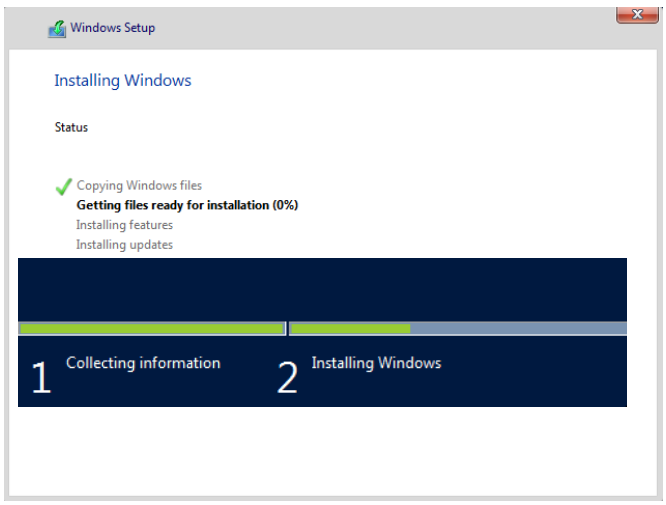

Windows Setup
Windows Server 2016
Install now
Repair your computer
© 2016 Microsoft Corporation. All rights reserved.

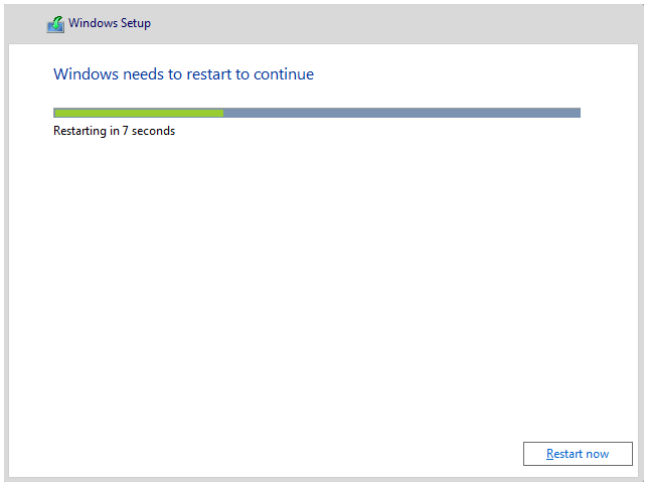

Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard
x64
11/21/2016
Windows Server 2016 Standard (Desktop Experience)
x64
11/21/2016
Windows Server 2016 Datacenter
x64
11/21/2016
Windows Server 2016 Datacenter (Desktop Experience)
x64
11/21/2016
Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."
Next

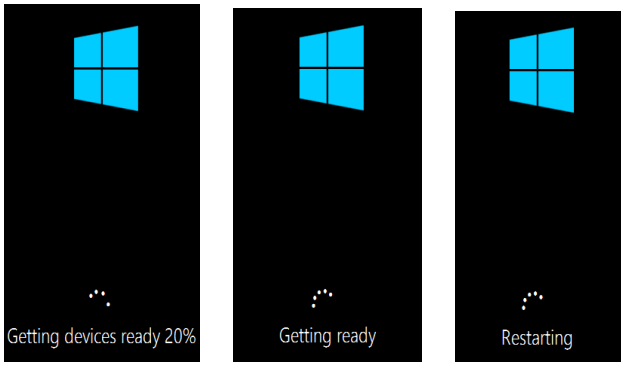

Windows Setup
Applicable notices and license terms
Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.
EULAID:T1S_SR_1_ED_SRVSTD_V_en-us
I accept the license terms
Next

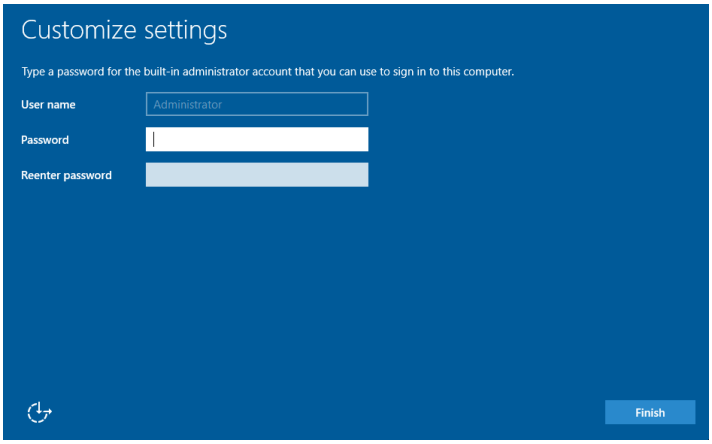

Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
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.
Help me decide


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


Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (0%)
Installing features
Installing updates
1
Collecting information
2
Installing Windows


Windows Setup
Windows needs to restart to continue
Restarting in 7 seconds
Restart now


Getting devices ready 20%
Getting ready
Restarting

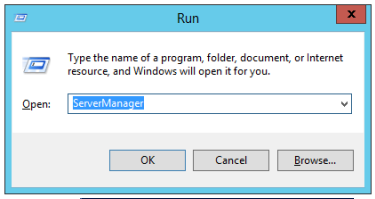

Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish

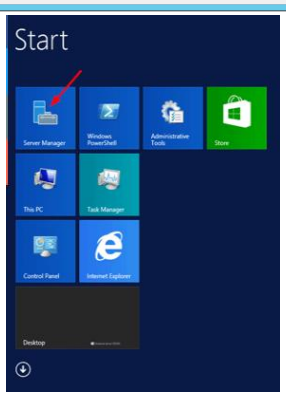

Press Ctrl+Alt+Delete to unlock
9:16
Monday, September 11

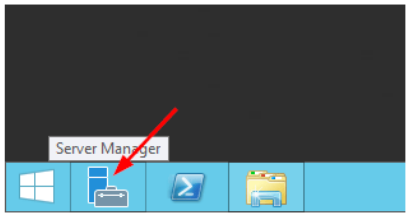

Administrator
Password

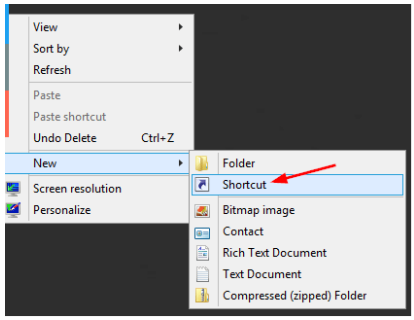
Windows Server 2016 Management

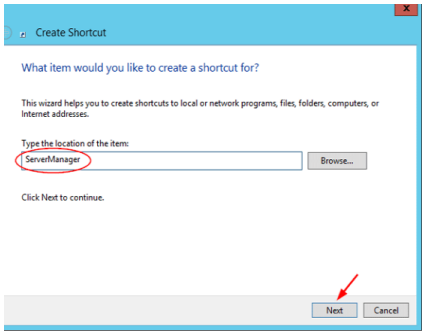
Windows Server 2016 Initial setup

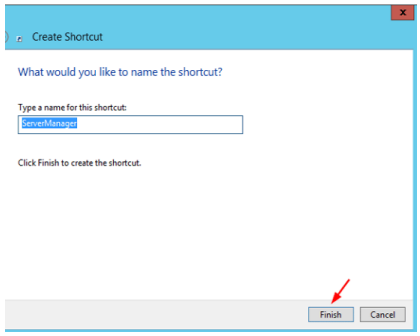


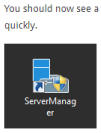




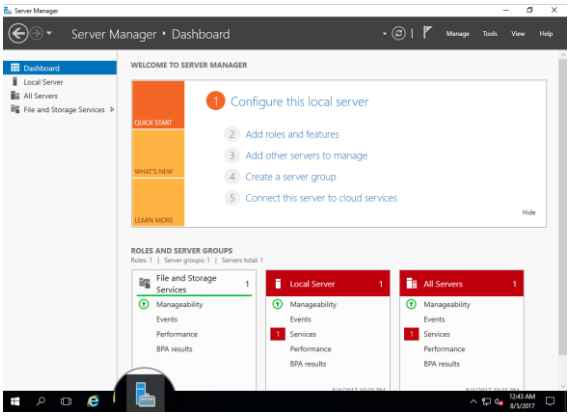


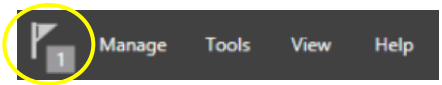




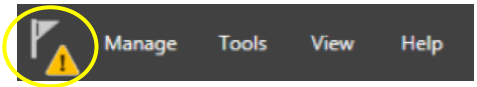


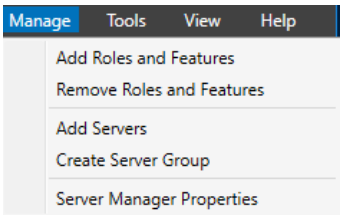
The Server Manager Dashboard screen provides, at a glance, all roles installed on the server, and will notify you of any errors or concerns. It also offers a Quick Start menu of hyperlink options.

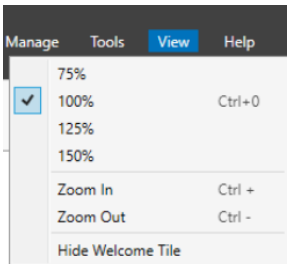


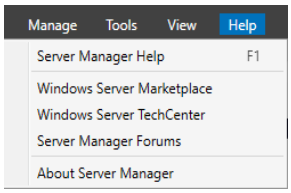


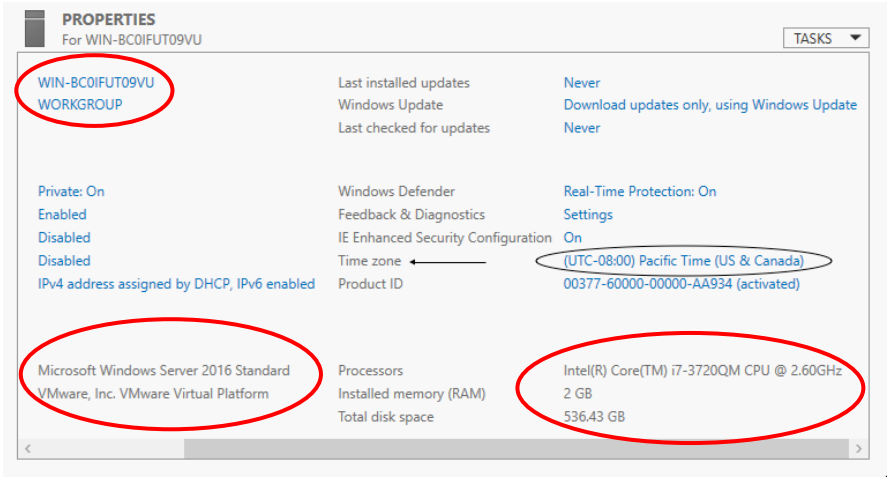
- The Notifications Area:
- The flag icon represents the Notifications Area and will display Task Details that are in progress, pending, or require additional actions. A number beside this icon indicates there are pending messages.
- If a Warning Triangle appears this means there are pending tasks that require your immediate attention.

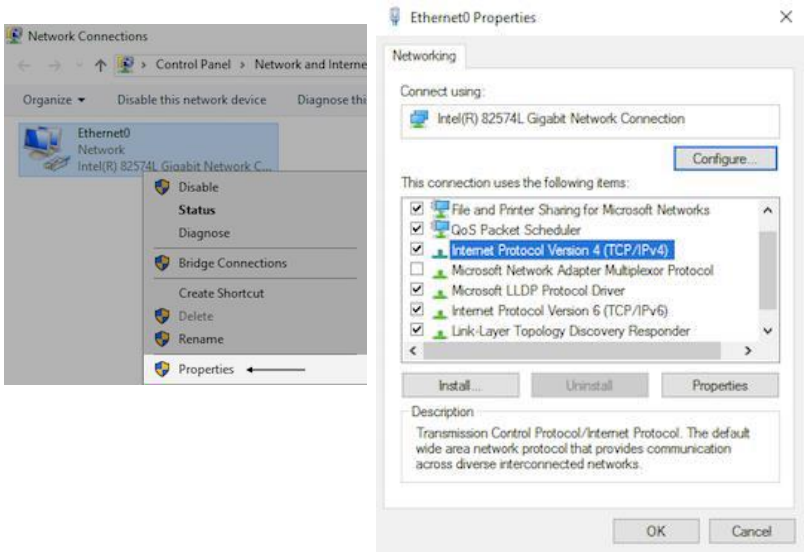


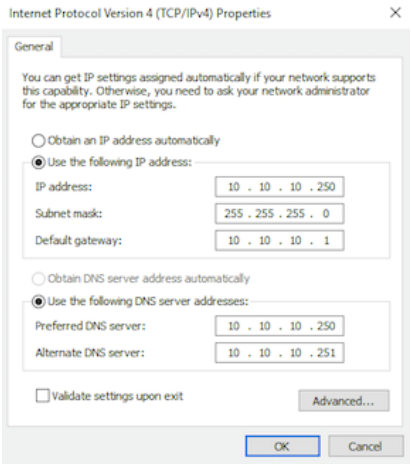


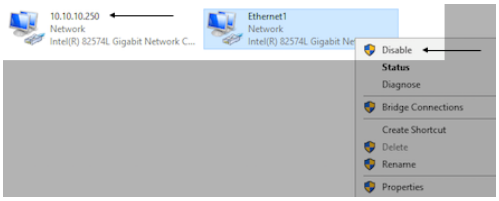


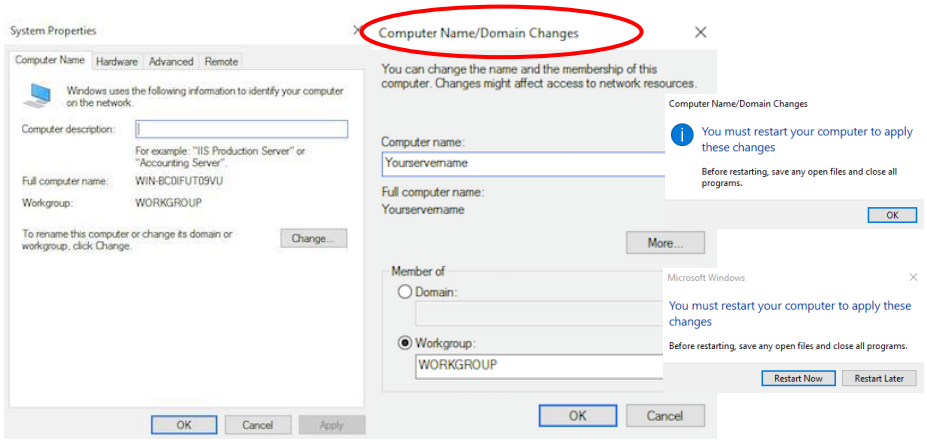


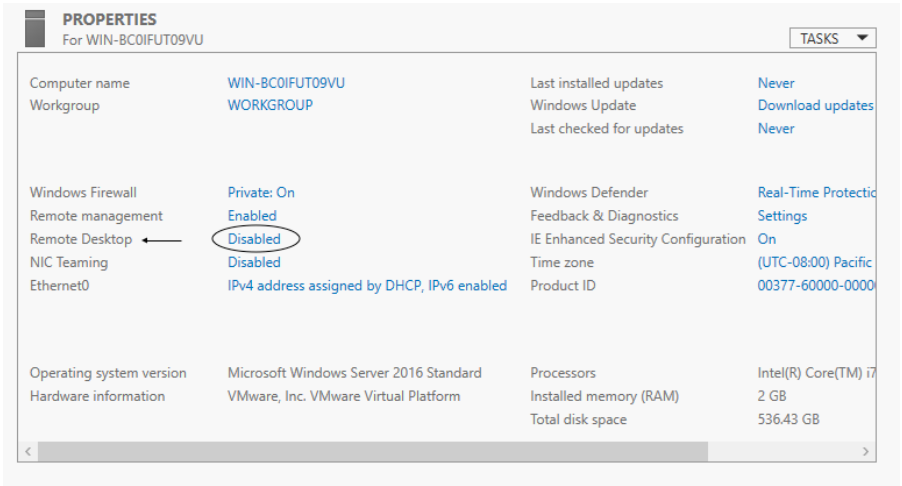

PROPERTIES
For WIN-BC0IFUT09VU
TASKS
WIN-BC0IFUT09VU
WORKGROUP
Last installed updates
Windows Update
Last checked for updates
Never
Download updates only, using Windows Update
Never
Private: On
Enabled
Disabled
Disabled
IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender
Feedback & Diagnostics
IE Enhanced Security Configuration
Time zone
Product ID
Real-Time Protection: On
Settings
On
(UTC-08:00) Pacific Time (US & Canada)
00377-60000-00000-AA934 (activated)
Microsoft Windows Server 2016 Standard
VMware, Inc. VMware Virtual Platform
Processors
Installed memory (RAM)
Total disk space
Intel(R) Core(TM) i7-3720QM CPU @ 2.60GHz
2 GB
536.43 GB

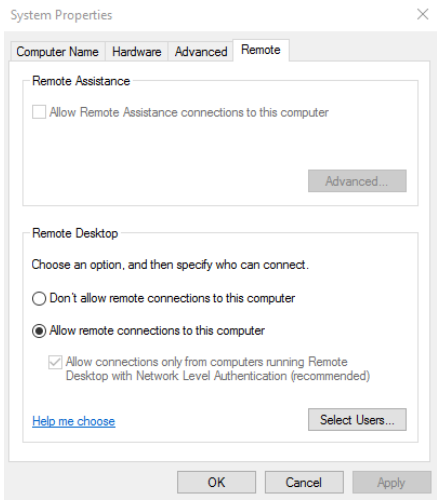

Network Connections
Control Panel
Network and Interne
Organize
Disable this network device
Diagnose thi
Ethernet0
Network
Intel(R) 82574L Gigabit Network C...
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
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)
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

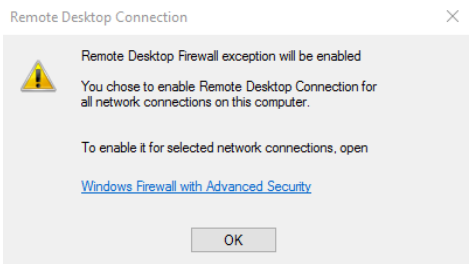

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 10 . 250
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 10 . 250
Alternate DNS server: 10 . 10 . 10 . 251
Validate settings upon exit
Advanced...
OK
Cancel

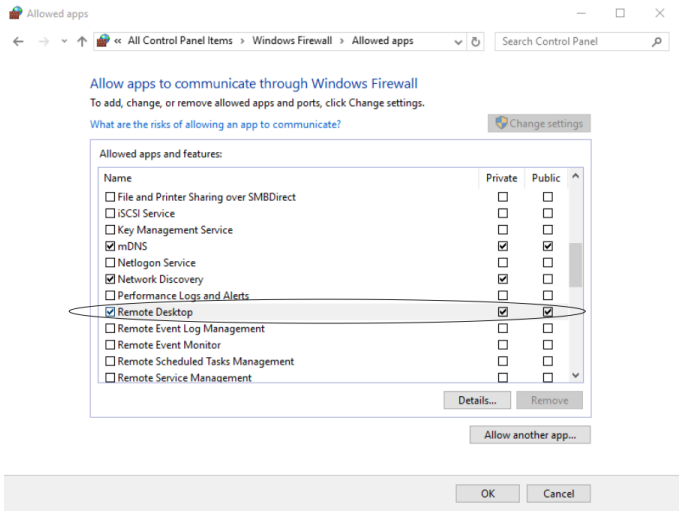

10.10.10.250
Network
Intel(R) 82574L Gigabit Network C...
Ethernet1
Network
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties


System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name: WIN-BC0IFUT09VU
Workgroup: WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
Yourservername
Full computer name:
Yourservername
More...
Member of
Domain:
Workgroup:
WORKGROUP
OK
Cancel
Computer Name/Domain Changes
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
OK
Microsoft Windows
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
Restart Now
Restart Later


PROPERTIES
For WIN-BC0IFUT09VU
TASKS
Computer name
WIN-BC0IFUT09VU
Workgroup
WORKGROUP
Last installed updates
Never
Windows Update
Download updates
Last checked for updates
Never
Windows Firewall
Private: On
Remote management
Enabled
Remote Desktop
Disabled
NIC Teaming
Disabled
Ethernet0
IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender
Real-Time Protectic
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC-08:00) Pacific
Product ID
00377-60000-0000
Operating system version
Microsoft Windows Server 2016 Standard
Hardware information
VMware, Inc. VMware Virtual Platform
Processors
Intel(R) Core(TM) i7
Installed memory (RAM)
2 GB
Total disk space
536.43 GB


System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply


Remote Desktop Connection
Remote Desktop Firewall exception will be enabled
You chose to enable Remote Desktop Connection for all network connections on this computer.
To enable it for selected network connections, open
Windows Firewall with Advanced Security
OK



- Roles - Roles are sets of software programs that when installed and configured properly, function automatically to provide multiple users and/or computers with access to resources within a network.
- Examples: DHCP, Active Directory & DNS, File Services, Print Server Services, etc. Roles typically include their own databases, can queue requests or record information about the network participants.
- One or more roles can be installed on a server depending on the capabilities of the hardware.

- Role Services – Role Services are software programs that add functionality to the role. Some Roles only have one specific function and do not have additional Role Services to choose from. Other Roles require a certain set of Role Services, which are installed without selection options.

- Features – Features are optional software programs that can be installed without direct correlation to available and regardless selected Roles.

- Functions - Functions are secondary or supporting features to the primary Roles that can be installed. Defining the Server management or administrative management functions (MMC), backing up files.

- AD DS – Active Directory Domain Services is the directory services database for Windows Server, used to process logons, authentication and directory searches. Installed on a domain controller, it manages communications across users and domains.

Active Directory Domain Services(ADDS)

- ADDS is a database and service.
- AD DS – Active Directory Domain Services is the directory services database for Windows Server, used to process logons, authentication and directory searches.
- Installed on a domain controller, it manages communications across users and domains.

- Active directory service store all the information needed to use and manage objects in a centralized location, simplifying the process of locating and managing these resources.
- Like telephone directory Active directory stores all objects information for effective and efficient centralized management.

ADDS

- Centralized data store – All the data in Active directory resides in a single distributed data repository(ntds.dit), allowing users easy access to the information from any location.
- A single distributed data store requires less administration and improves the availability and organization of data.
- Scalability – Active directory enables you to scale the directory to meet business and network requirements.
- ADDS allows millions of objects per domain and uses indexing technology and advanced replication techniques to speed the performance.

ADDS

- Extensibility – The structure of Active Directory database(schema) can be expanded to allow customized type of information.
- Manageability – Since it is a centralized single database, AD can be managed with less administrative efforts.
- AD is integrated with DNS. Active directory and DNS uses same hierarchical structure. AD clients use DNS to locate domain controllers.
- AD provides Policy based administration
- Flexible secure authentication and authorization
- Security integration

ADDS Features

- ✓ADDS is a database and service.
- ✓ADDS stores all it's object information's, like users, groups, computers, printers, shared folders, Ous, contacts etc…
- ✓ADDS provides centralized network administration
- ✓ADDS offers domain model networking
- ✓Easy to manage a large network
- ✓Highly secured environment
- ✓It is scalable as per business requirement
- ✓ADDS provides log on authentication, security policies
- ✓Since it maintains a single centralized database, objects searching and management is very easy
- ✓ADDS is integrated with DNS. Active directory and DNS uses same hierarchical structure. AD clients use DNS to locate domain controllers.

Active Directory

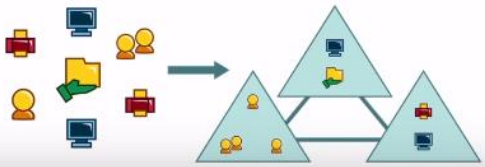
How Directory Service works?

- AD uses LDAP (Open Source), Kerberos and DNS

LDAP	It is a standard application protocol. It help us to access and maintain directory information service via network
Kerberos	It is computer network authentication protocol. It provides authentication service over network
DNS	Domain name service . It helps to translate IP to name or name to IP.

What is Active Directory?

- Is similar to a telephone directory
- It is a software to arrange, store information; provides access and permissions based on those information



What is Active Directory?

- Arranges all the Network's Users, Computers and other Objects into Logical, Hierarchical groupings
- Active Directory information is used to authenticate/ authorize the Users, Computers, Resources which are part of a network

What is Active Directory?

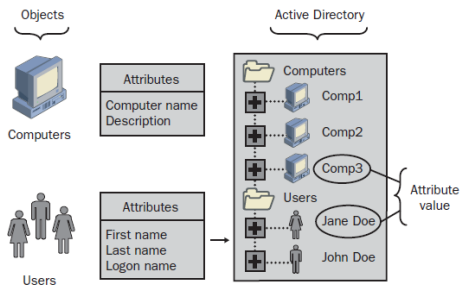
- Has information about all the objects - Users, Computers, Resources like Printers, Shared Files/ Folders - in an organization's network.

Active Directory Objects

- Physical entities of a network
- Can be described by a subset of attributes
- Objects
  - Forest
  - Domain
  - Organizational Unit
  - User
  - Group
  - Contact
  - Computer
  - Shared folder
  - Printer
  - Site
  - Subnet

ADDS Objects and Attributes

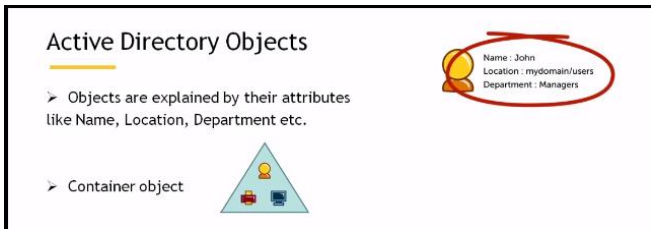
- The data stored in Active Directory, such as information about users, printers, servers, databases, groups, computers, and security policies, is organized into objects.
- An *object* is a distinct named set of attributes that represents a network resource. Object attributes are characteristics of objects in the directory.

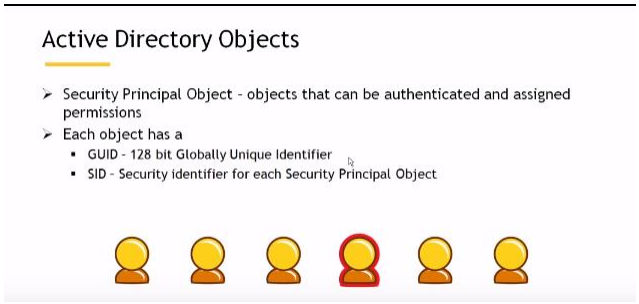


Active Directory Schema

- The Active Directory schema defines objects that can be stored in Active Directory. The *schema* is a list of definitions that determines the kinds of objects and the types of information about those objects that can be stored in Active Directory.
- The schema is defined by two types of objects: schema class objects (also referred to as schema classes) and schema attribute objects (also referred to as schema attributes).
- Schema class objects and attribute objects are collectively referred to as schema objects or metadata.

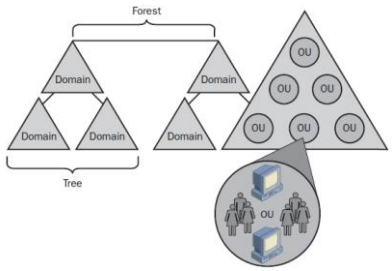
- *Schema class objects* describe the possible Active Directory objects that can be created.
- *Schema attribute objects* define the schema class objects with which they are associated.





Logical Structures

- In Active Directory, you organize resources in a logical structure—a structure that mirrors organizational models—using domains, OUs, trees, and forests. Grouping resources logically allows you to easily find a resource by its name rather than by remembering its physical location.



ADDS - Domain

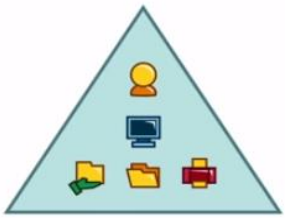
- Domain – The core unit of logical structure in Active Directory is the domain, which store millions of objects. Objects stored in a domain are considered vital to the network.
- Active Directory is made up of one or more domains. A domain can span more than one physical location. All network objects exists within a domain, and each domain stores information only about the objects that it contains.

ADDS-Domain

- A domain is a security boundary. Access to domain objects is governed by access control lists(ACLs), which contains the permissions associated with the objects.
- None of the security policies and settings-such as administrative rights, security policies and ACLs can cross from one domain to another domain.
- A domain administrator has absolute rights to set policies only within their domain.

Domain

- If a user has access to a domain, he can logon from anywhere and any computer in that domain.



Domain

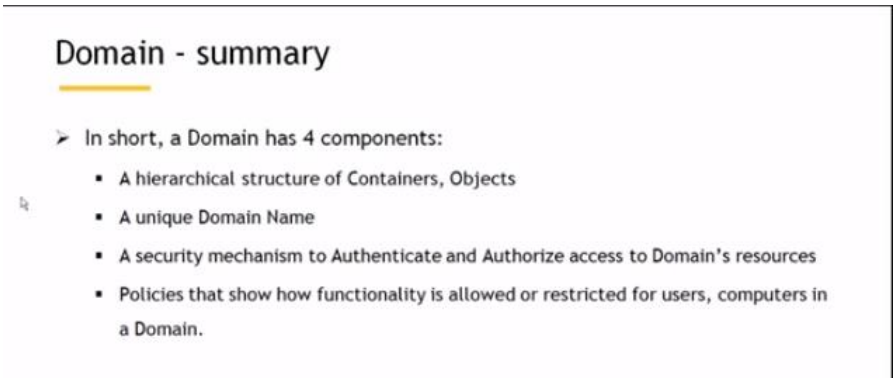
- Domain controller is responsible for all the authentications, authorizations, additions, deletions, edits, modifications inside a domain.

Domain

- If a user has access to a domain, he can logon from anywhere and any computer in that domain.

Domain

- The permissions, policies and rights can be set for all the objects at the domain level or at the individual object level as well.

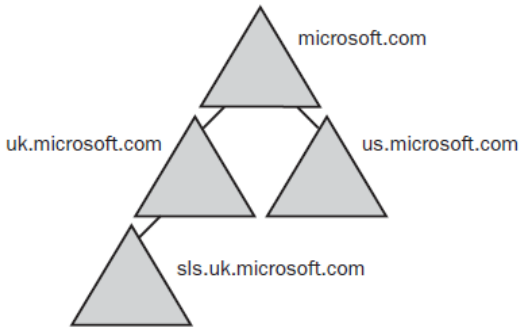


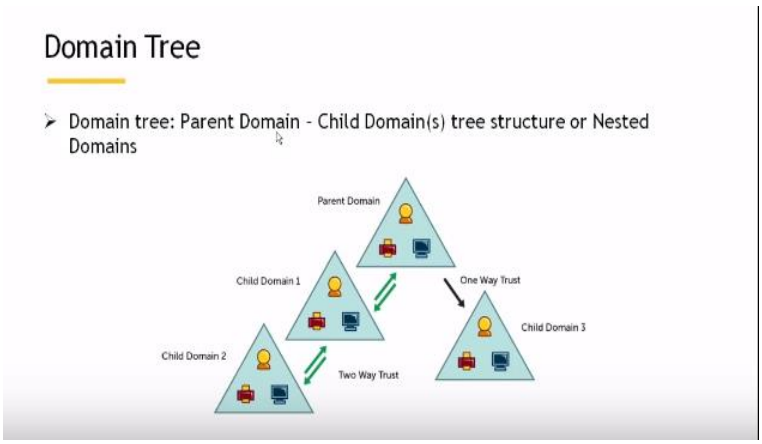
Domain - TREE

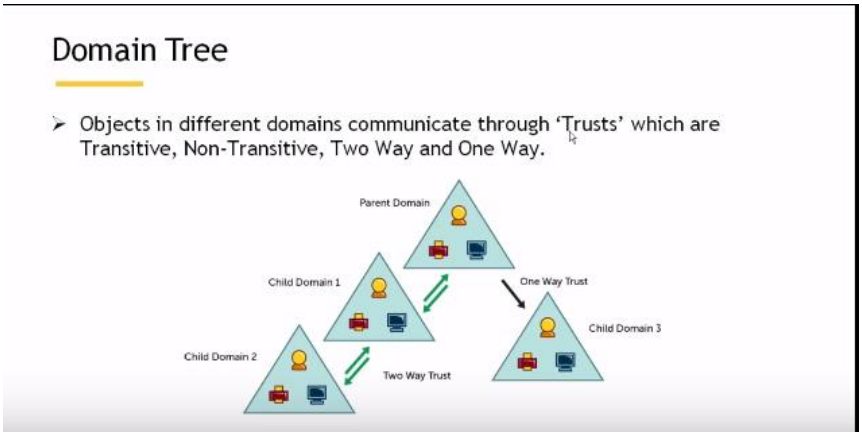
- Tree is a grouping or hierarchical arrangement of one or more domains that you can create by adding one or more child domains to an existing parent domain.
- Domains in a tree shares a contiguous name space and hierarchical name structure. By creating hierarchy domains in a tree you can retain security and allow administration within OU or within a single domain of a tree.

Domain - TREE

- Following DNS structure the domain name of a child domain is the relative name of that child domain appended with the name of the parent domain.

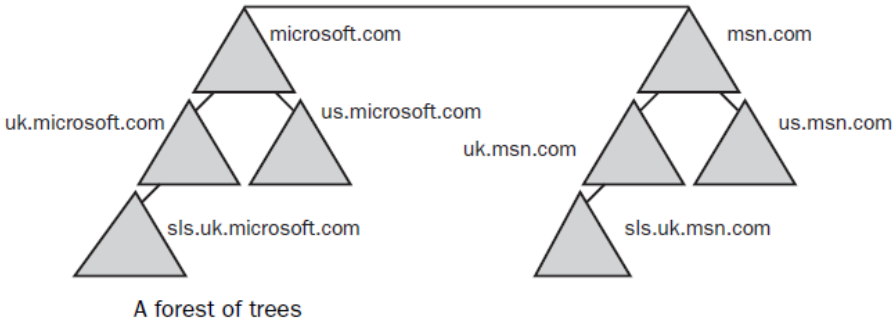






ADDS - FOREST

- A forest is a grouping or hierarchical arrangements of one or more separate, completely independent domain trees.
- All domains in forest share a common schema
- All domains in a forest share a common Global Catalog
- All domains in a forest are linked by implicit two-way transitive trust
- Trees in a forest have different naming structure according to their domains.
- Domains in a forest operate independently, but the forest enables communication across the entire organization.

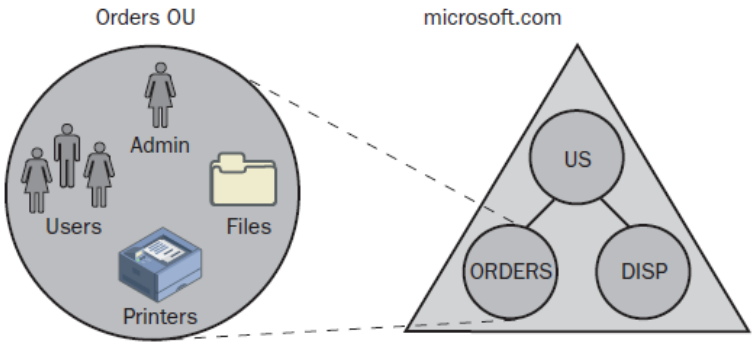


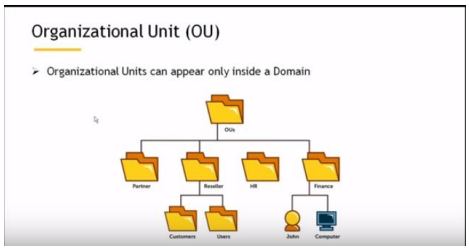
A forest of trees

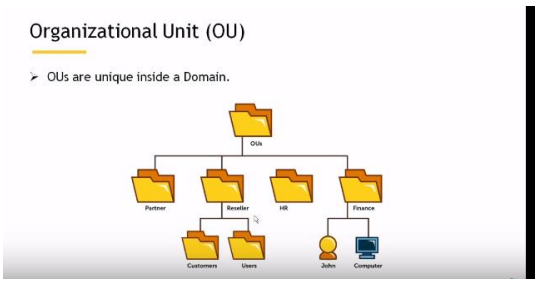
ADDS - Organizational Unit (OU)

- An OU is a container used to organize objects within a domain into logical administrative groups. An OU can contain objects such as user accounts, groups, computers, printers, applications, file shares and other OUs from the same domain.
- An OU can have many sub-OUs
- An OU can be delegated with separate administrative authority, by adding OUs to other OUs or nesting, you can provide administrative control in hierarchical fashion.
- An OU is the smallest administrative unit in an AD domain

ADDS - OU

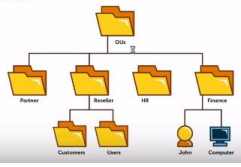

Orders OU
microsoft.com
Admin
Users
Files
Printers
US
ORDERS
DISP


Organizational Unit (OU)
Organizational Units can appear only inside a Domain
OUs
Partner
Reseller
HR
Finance
Customers
Users
John
Computer


Organizational Unit (OU)
OUs are unique inside a Domain.
OUs
Partner
Reseller
HR
Finance
Customers
Users
John
Computer

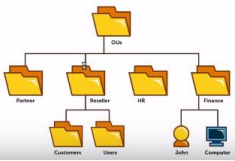
Organizational Unit (OU)

- Contains other objects like Users, Groups, Contacts, Computers, Printers, Shared folders etc.



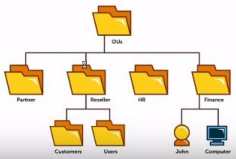
Organizational Unit (OU)

- An OU can contain another OU(s).



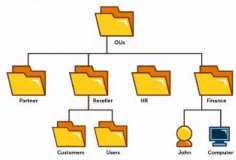
Organizational Unit (OU)

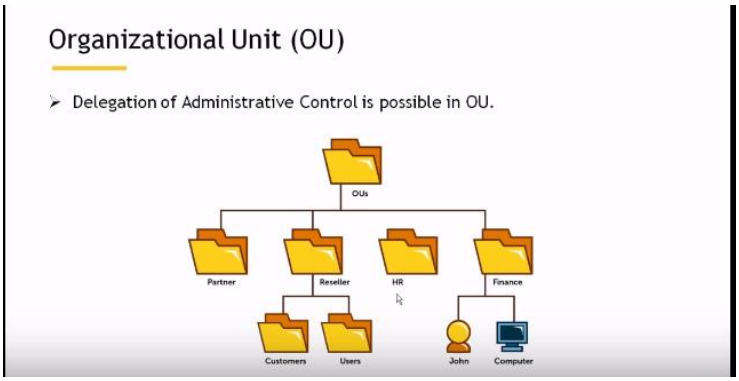
- Nested OUs have Parent-Child relationship.



Organizational Unit (OU)

- Group Policy Settings can be set at the OU level.





ADDS – Physical Components

- Physical components of Active Directory are Domain Controllers and Sites.
- Domain Controller (DC) – DC is a computer running windows server OS added active directory domain services, that stores a replica of the domain directory (Database).
- A domain can have one or more domain controllers. A domain controller can serve only one domain.
- A domain controller can authenticates user logon attempts and maintains the security policy for a domain.

ADDS – Physical Components

- Each DC stores complete copy of all Active Directory information for that domain, manages changes to that information and replicates those changes to other DCs in the same domain.
- DCs in a domain automatically and immediately replicate directory information for all objects in the domain to each other.
- ADDS uses multi master replication, in which no one DC is the master , instead all DCs within a domain are peers.

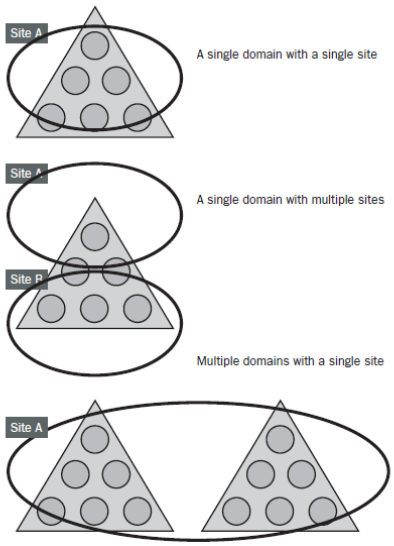
ADDS – Physical Components

- Having more than one DC provides fault tolerance in a domain.
- DC manages all aspects of users domain interactions such as locating domain objects, user logon attempts and security policy settings for domain objects.

ADDS - SITE

- Sites - A *site* is a combination of one or more IP subnets connected by a highly reliable and fast link to localize as much network traffic as possible. Typically, a site has the same boundaries as a local area network (LAN).
- When you group subnets on your network, you should combine only subnets that have fast, cheap, and reliable network connections with one another.

SITE



ADDS – Global Catalog

- ADDS allows users and administrators to find objects such as users, groups, printers, file, folders in their own domain. However finding objects outside the domain and across the enterprise requires a separate mechanism that allows the domains to act as one entity.
- A catalog service contains selected information about every object in all domains in the directory, which is useful in performing searches across an enterprise.
- The global catalog is the catalog service provided by Active Directory.

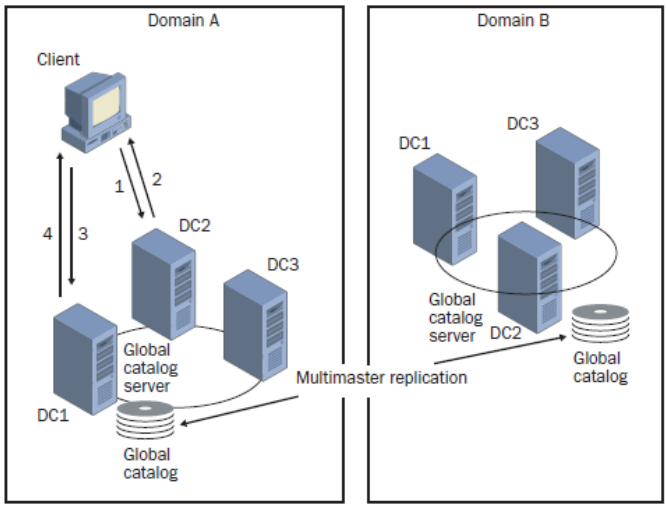
ADDS – Global Catalog

- A global catalog is the central repository of information about all objects in a tree or forest. By default global catalog is created in the first domain controller in a forest.
- A domain controller holds a copy of the catalog is called global catalog server. You can delegate any DC in a forest as a global catalog server.

ADDS – Global Catalog

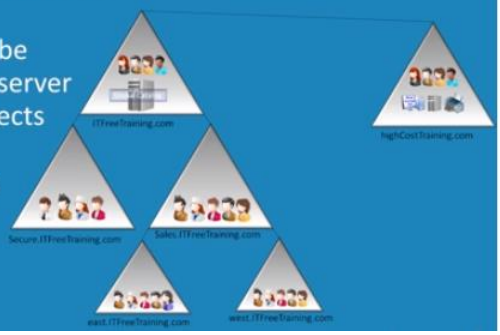
- Global catalog stores a full replica of all objects attributes in the directory for its host domain and a partial replica of all objects attributes contained in the directory for every other domain in the forest.
- Main services of GC - 1. GC enables a user to log on to a network by providing universal group membership information to a domain controller when a logon process initiated.
- 2. GC enables finding directory information regardless of which domain in the forest actually contains the data.

Global Catalog



Global Catalog (GC)

Each domain has separate database
Acts as an index
Any domain controller can be made into a global catalog server
Contains a subset of all objects
All objects in the forest
Holds multi domain groups



Global Catalog Facts

Any domain controller can be a Global Catalog (GC)
Must have one GC per domain
Should have more than one for redundancy
Windows Server 2008 all DC's are GC's by default
Requires more disk space
Requires more bandwidth

Active Directory User

- Part of the organization
- Unique identity in the domain
- Accesses the domain's resources
- Authorization based access
- Has a unique SID
- Account is unique and is secured by a password

Active Directory Computer

- Individual Computers/ Workstations, Servers which are part of a network.
- Each computer has a unique computer account.
- Computer account allows each computer to be authenticated and authorized for access to the domain and domain resources.
- A server could be a Domain Controller or Global Catalog Server or a Member Server.

Active Directory Contact

- An individual who is not part of the organization but related to the organization. Example: Customer, Supplier, Vendor, etc.
- Unlike a user, a Contact cannot logon or access the domain or network.
- Cannot be assigned permissions or authorizations or restrictions.

Active Directory Group

- Contains Users and Computers who are called members of the group.
- All permissions, authorizations and restrictions placed on the groups apply to all the members of the group.
- Two types of groups

Security groups

Mail groups

Active Directory Group

- Group scopes
  - **Domain local** - To give access to resources in the same domain as the group, users can be from different domains.
  - **Global group** - To give access to resources that are in different domains to users from a specific domain.
  - **Universal group** - Used to give access to resources located in different domains to a group of users from different domains.

Why should we use Active Directory Services?

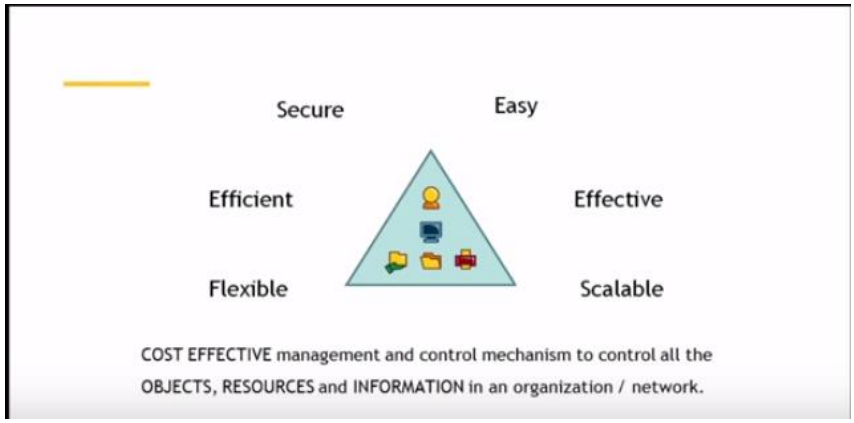
- Highly secure - Possible to have *layered security*. That is, have policies and permissions for security at different levels.
- Objects can be *located anywhere* physically, yet can securely access domain/network's resources.
- Millions of users can be added to a single domain. Highly scalable and readily extensible.
- Easy and efficient search mechanism to locate an object.

Why should we use Active Directory Services?

- **Centralized storage** for user information. This makes the process of backup and restore a lot more efficient.
- Serves as a platform for services like Exchange, Office365, SharePoint, etc.
- **Individual Profiles** - Users can have the same environmental settings immaterial of which computer or location they logon from.
- **Mandatory Profiles** - It is also possible to restrict/allow a specific set of applications and services to a set of users/groups.
- **Centralized Auditing** - makes it easier to track important security events.

Where can Active Directory Services be used?

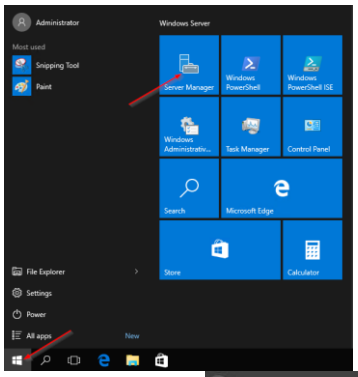
- Any organization that has a network setup.
- Organizations which require 24*7 uptime.
- Any organization where the number of users, computers, or resources will keep changing.
- Any organization where information/ data security is vital.
- Any organization that operates in multiple locations.

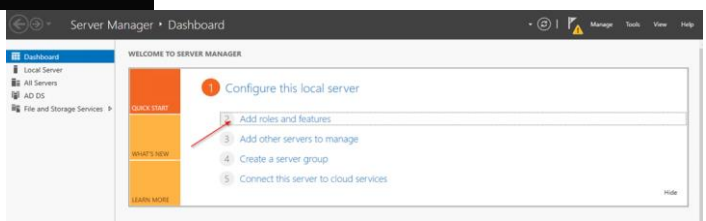


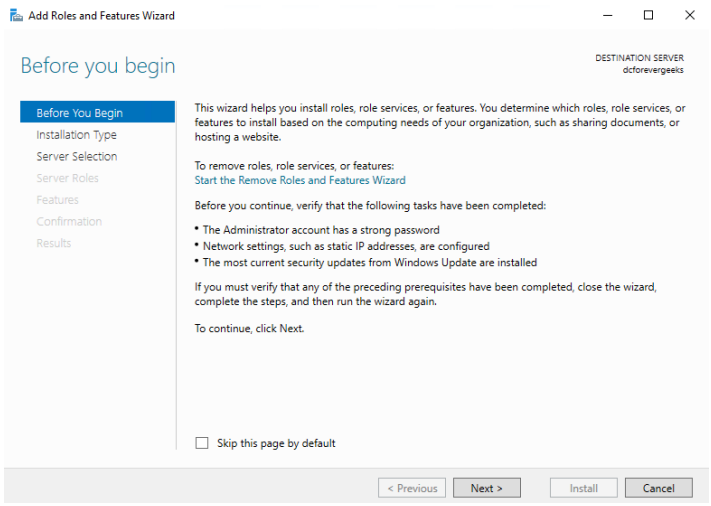
ADDS – Directory (NTDS.DIT)

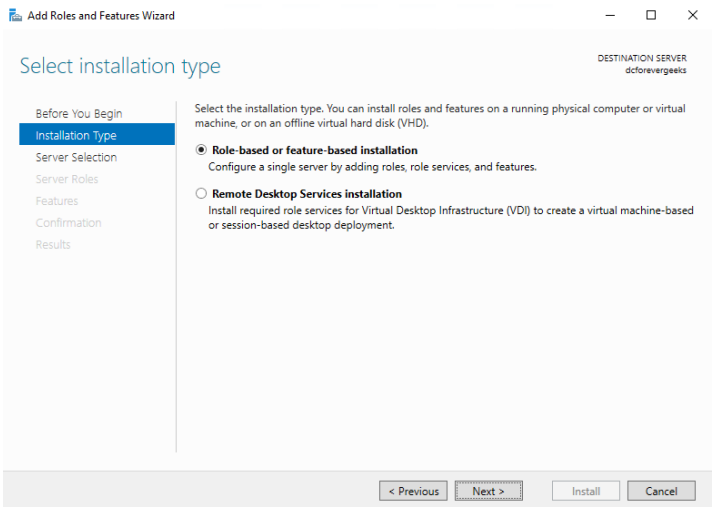
- The information stored in Ntds.dit file is logically partitioned into four categories. Each of these information categories is referred as a directory partition.
- Schema partition - This partition defines the objects that can be created in the directory and the attributes those objects can have. This data is common to all domains in a forest and is replicated to all domain controllers in a forest.

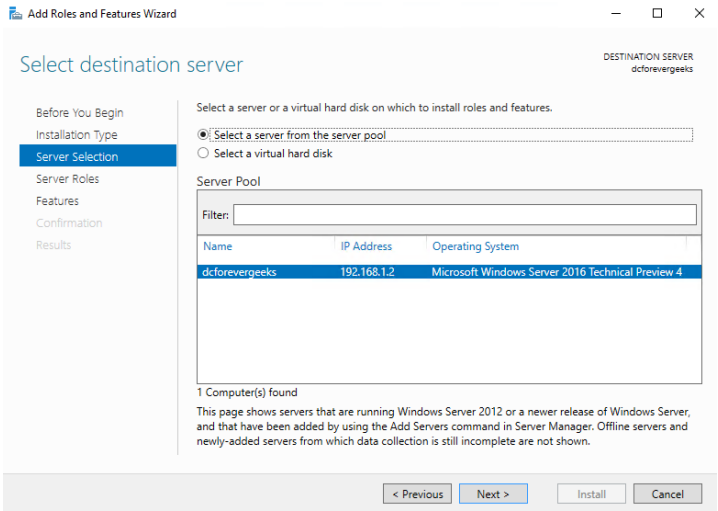
ADDS Installation

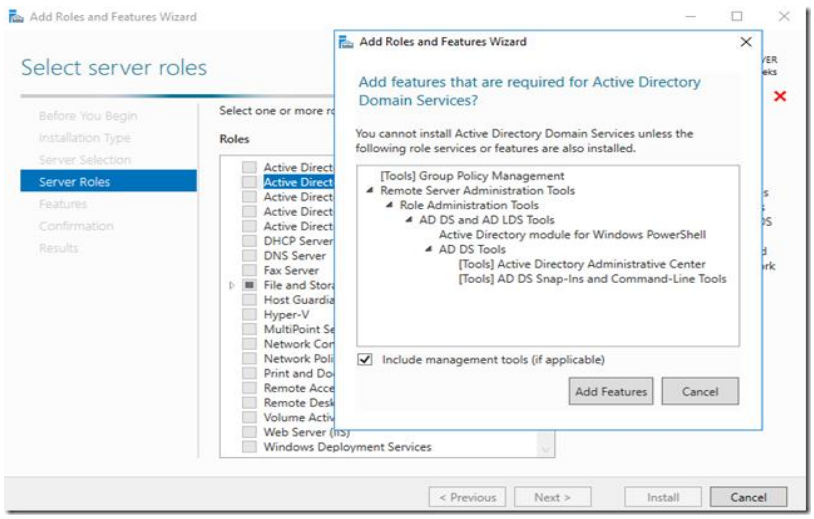


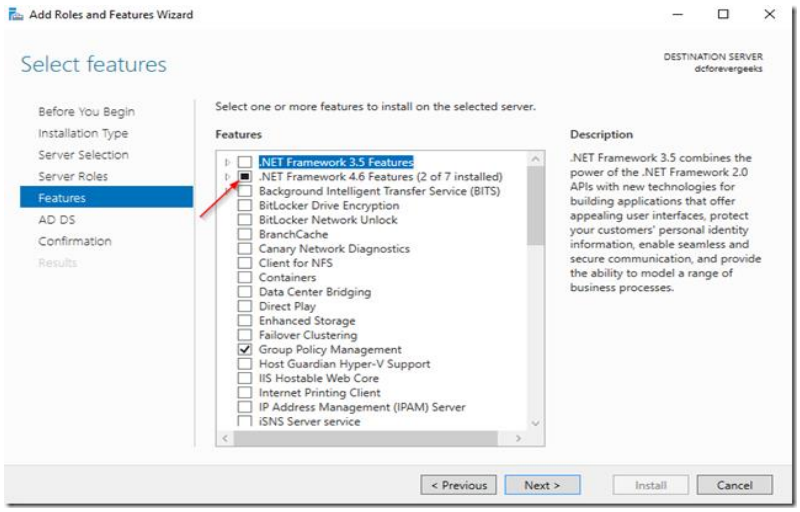


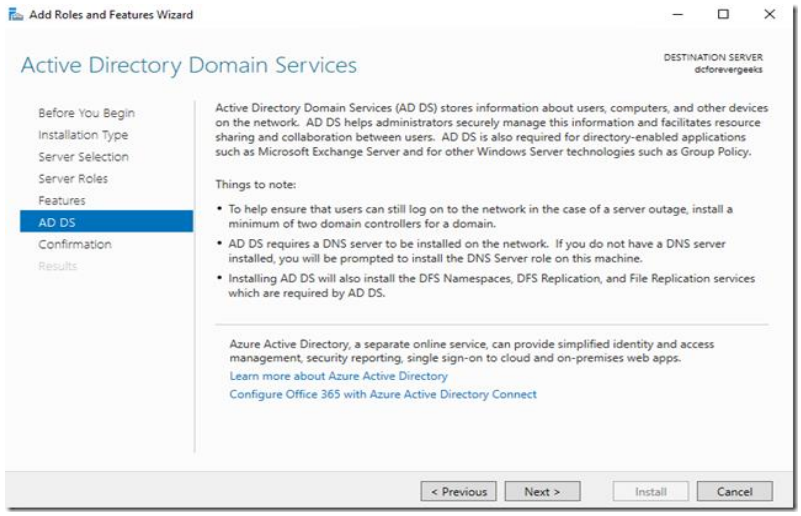

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install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

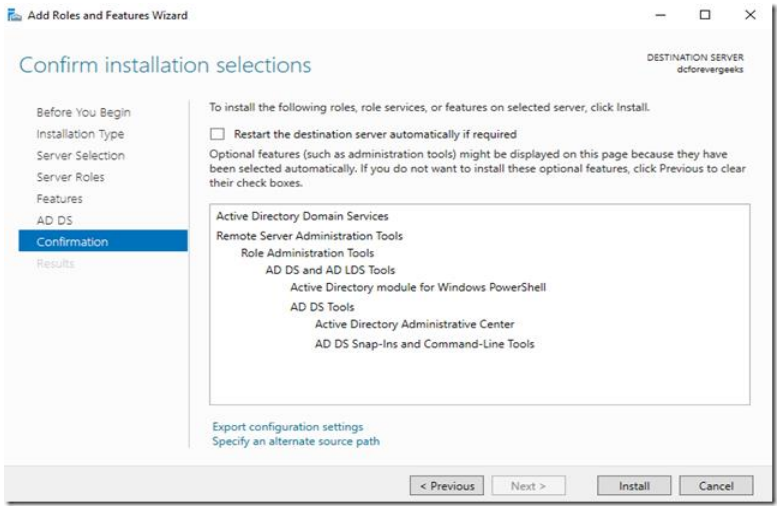

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or 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

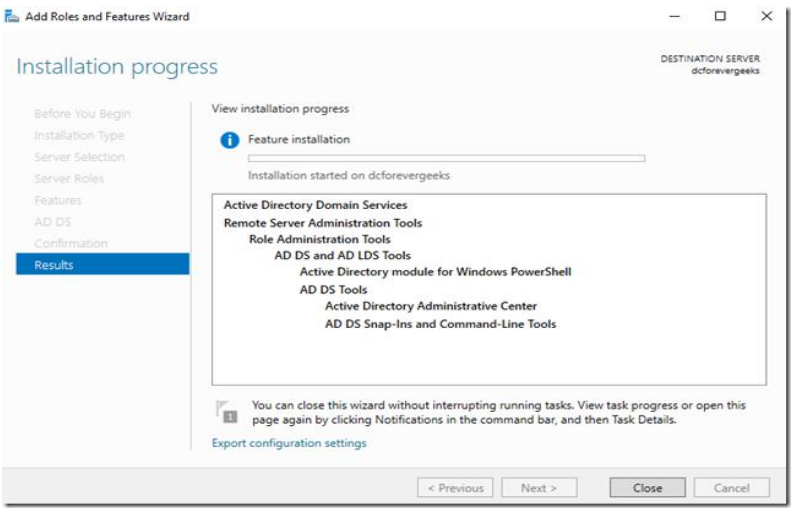

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
dcforevergeeks
192.168.1.2
Microsoft Windows Server 2016 Technical Preview 4
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

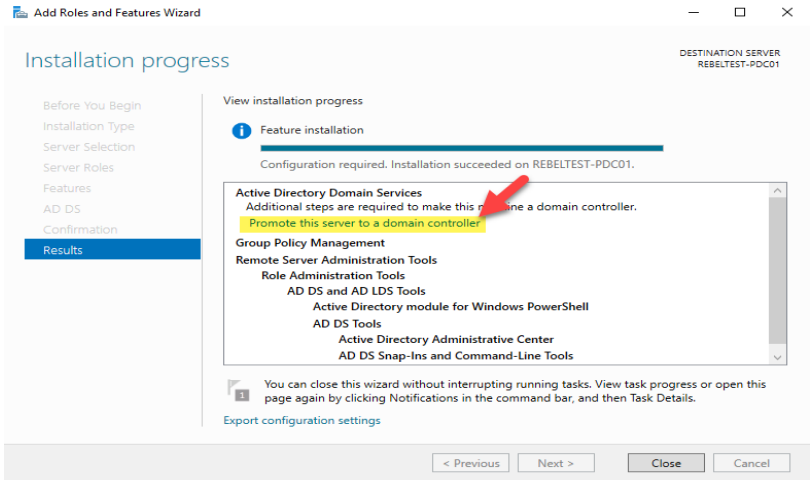

Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Roles
Windows Deployment Services
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active 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
< Previous
Next >
Install
Cancel

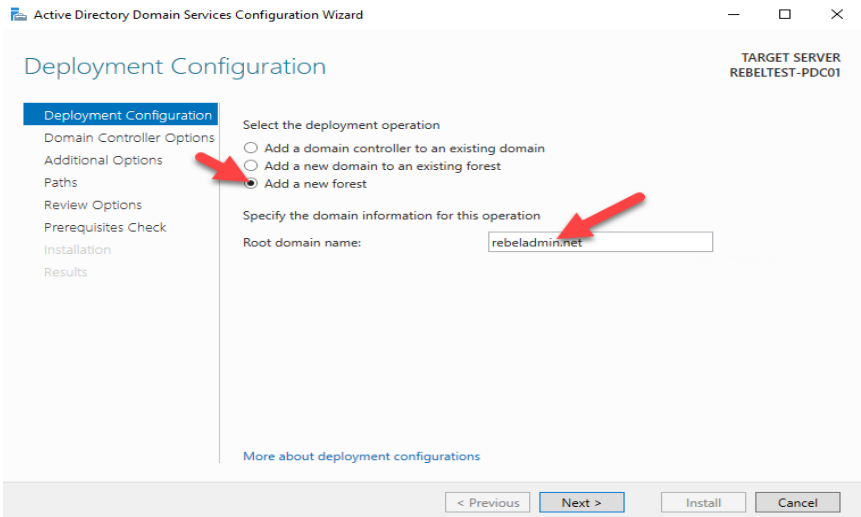

Add Roles and Features Wizard
Select features
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Canary Network Diagnostics
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
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

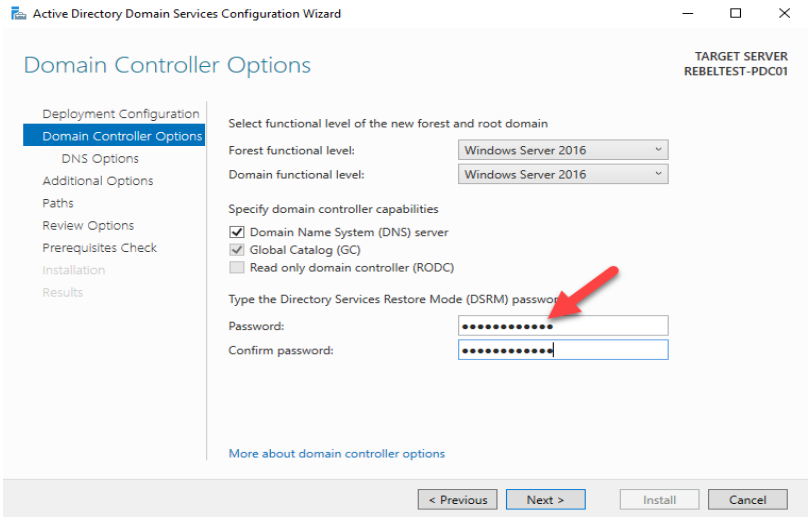

Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.
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.
• Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.
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

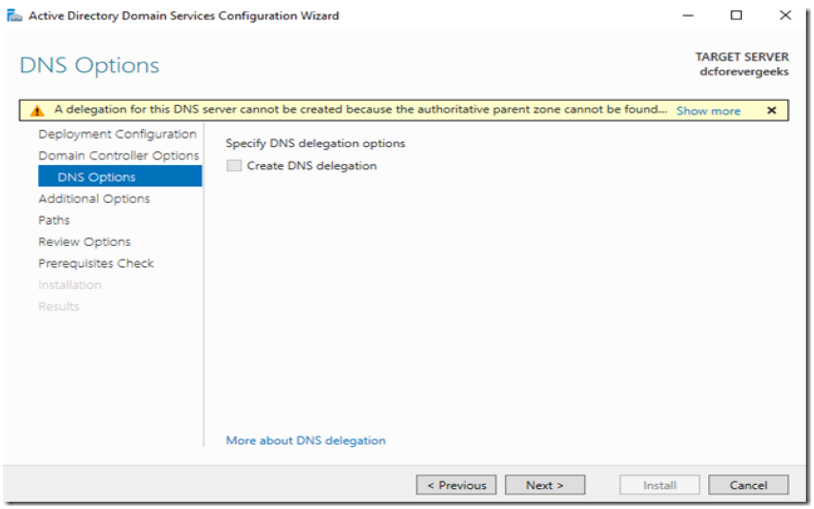

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the 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
Remote Server Administration Tools
Role Administration 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

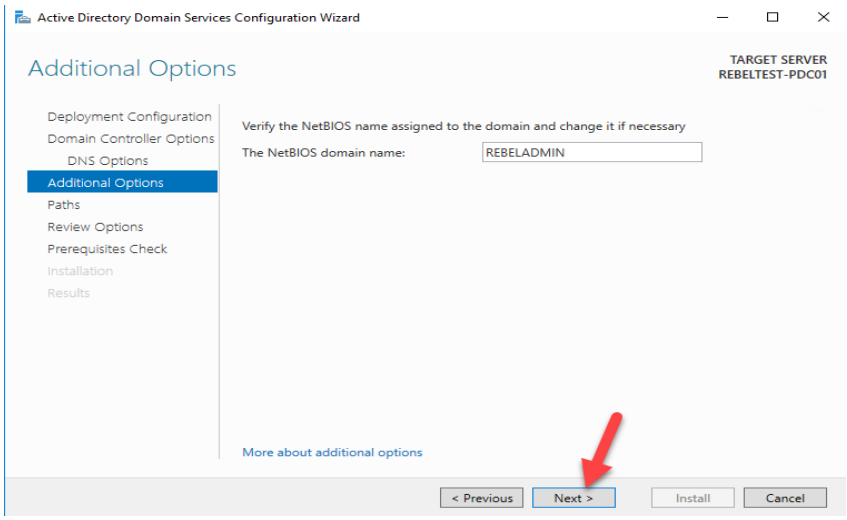

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
dcforevergeeks
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Installation started on dcforevergeeks
Active Directory Domain Services
Remote Server Administration Tools
Role Administration 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
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

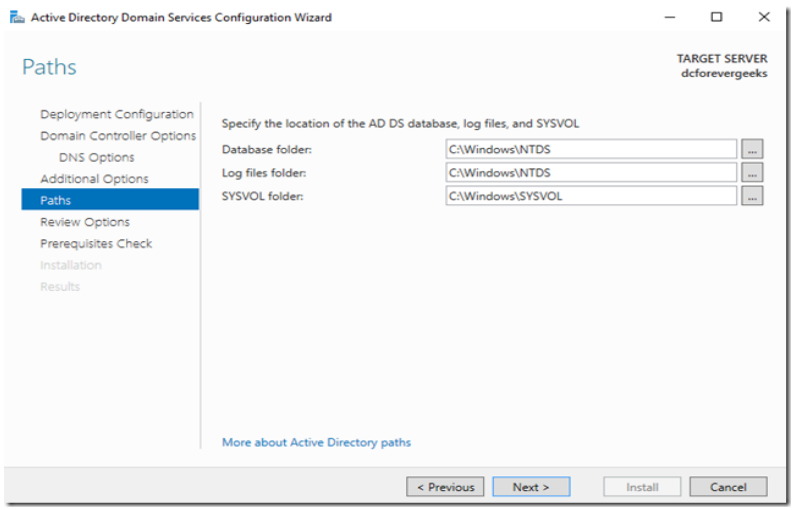

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
REBELTEST-PDC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on REBELTEST-PDC01.
Active Directory Domain Services
Additional steps are required to make this m ne a domain controller.
Promote this server to a domain controller
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
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line 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

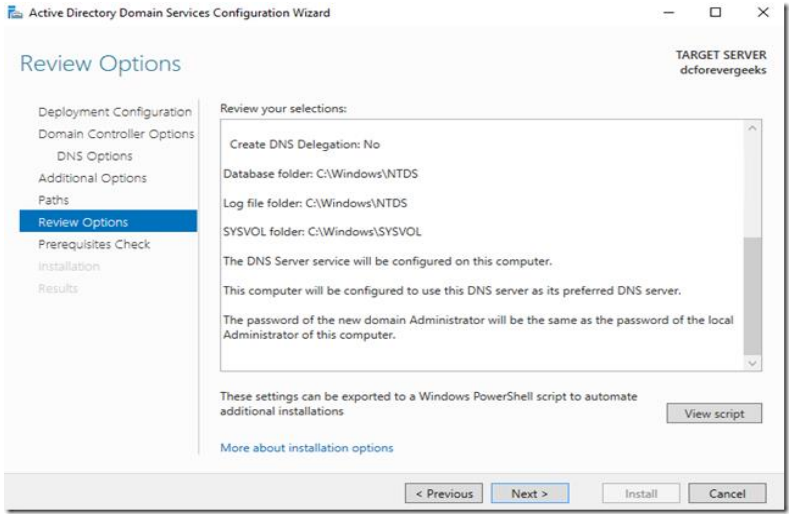

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
REBELTEST-PDC01
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
rebeladmin.net
More about deployment configurations
< Previous
Next >
Install
Cancel

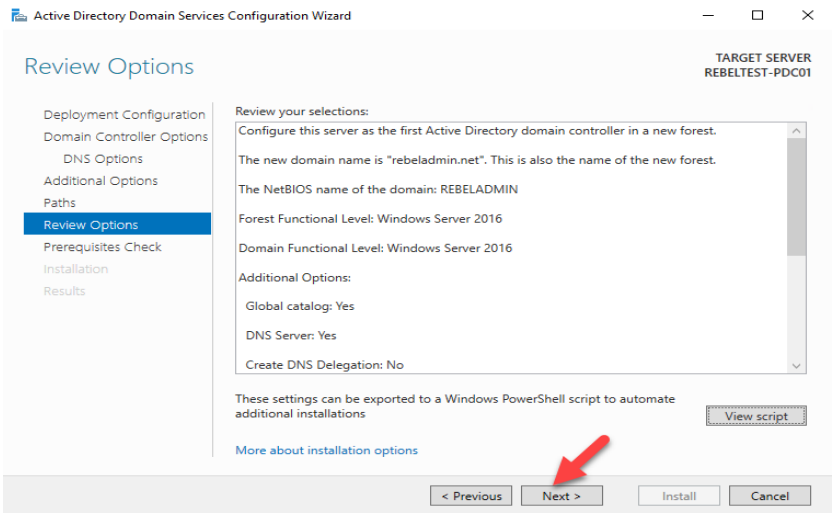

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
REBELTEST-PDC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root 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) passwor
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel

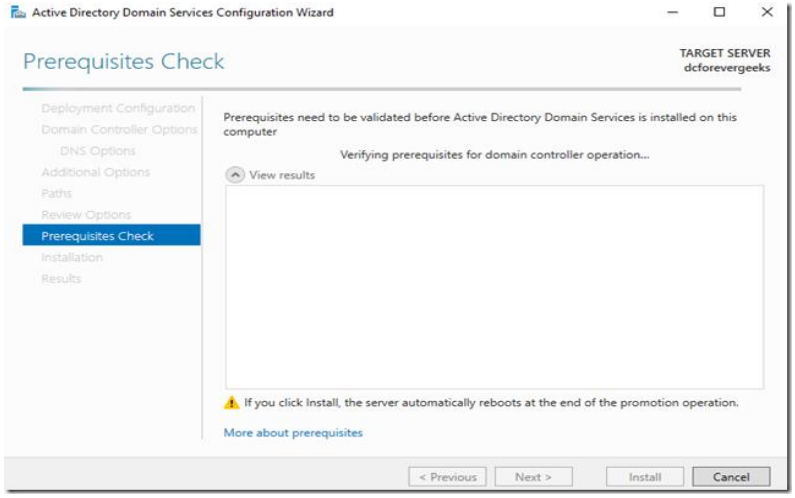

Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
dcforevergeeks
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel

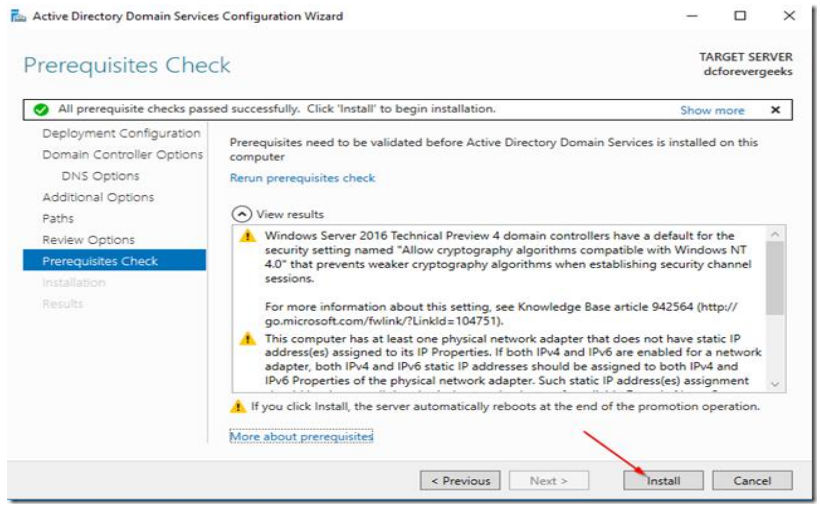

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
REBELTEST-PDC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
REBELADMIN
More about additional options
< Previous
Next >
Install
Cancel

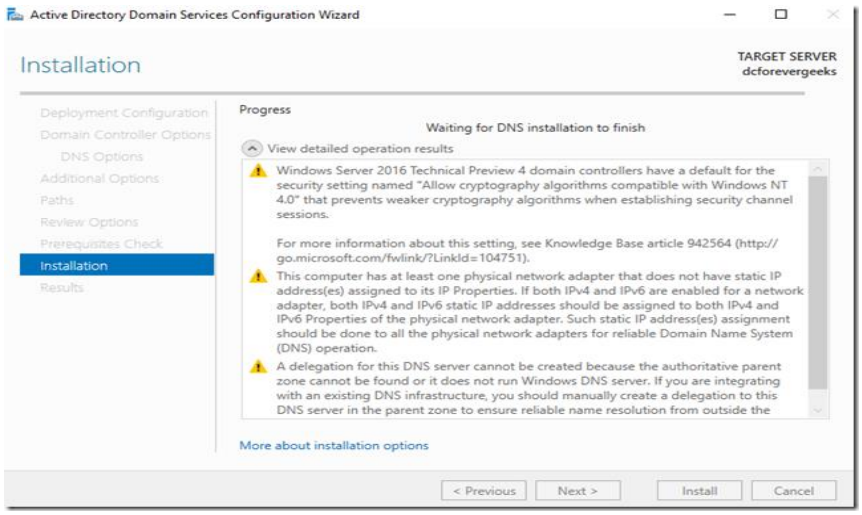

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
dcforevergeeks
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel

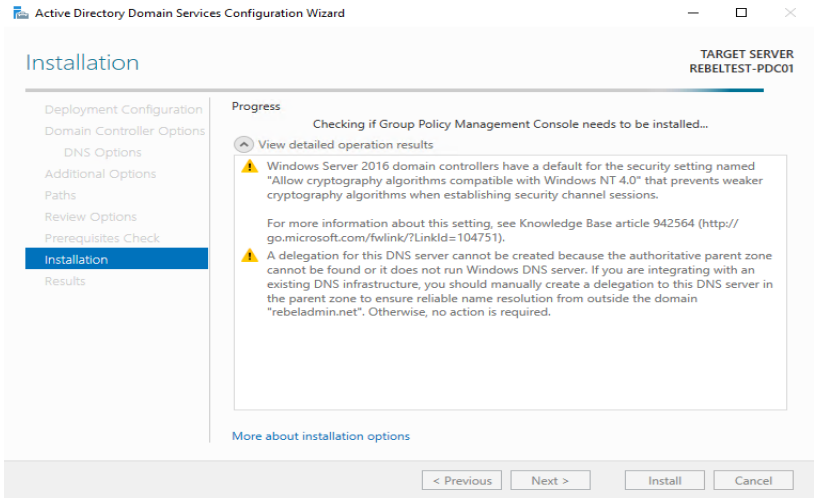

Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
dcforevergeeks
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Create DNS Delegation: No
Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel

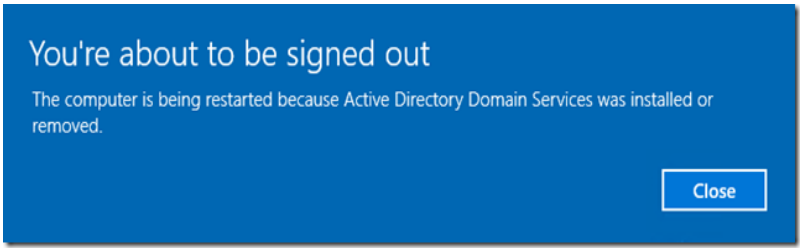

Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
REBELTEST-PDC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "rebeladmin.net". This is also the name of the new forest.
The NetBIOS name of the domain: REBELADMIN
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
dcforevergeeks
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
Verifying prerequisites for domain controller operation...
View results
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

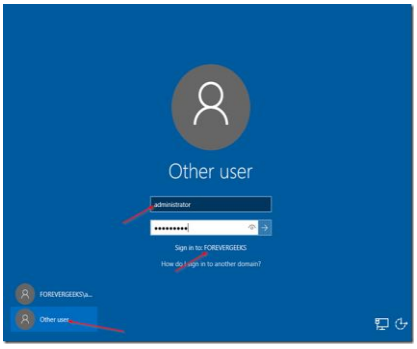

Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
dcforevergeeks
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites 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 2016 Technical Preview 4 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
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
dcforevergeeks
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Waiting for DNS installation to finish
View detailed operation results
Windows Server 2016 Technical Preview 4 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 (DNS) operation.
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the
More about installation options
< Previous
Next >
Install
Cancel

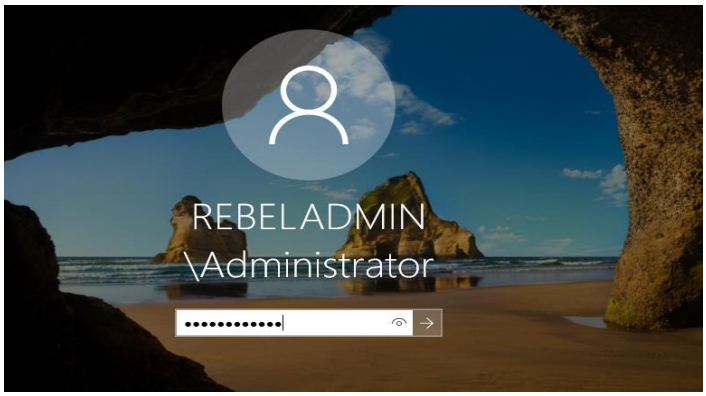

Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
REBELTEST-PDC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Checking if Group Policy Management Console needs to be installed...
View detailed operation results
Windows Server 2016 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).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "rebeladmin.net". Otherwise, no action is required.
More about installation options
< Previous
Next >
Install
Cancel

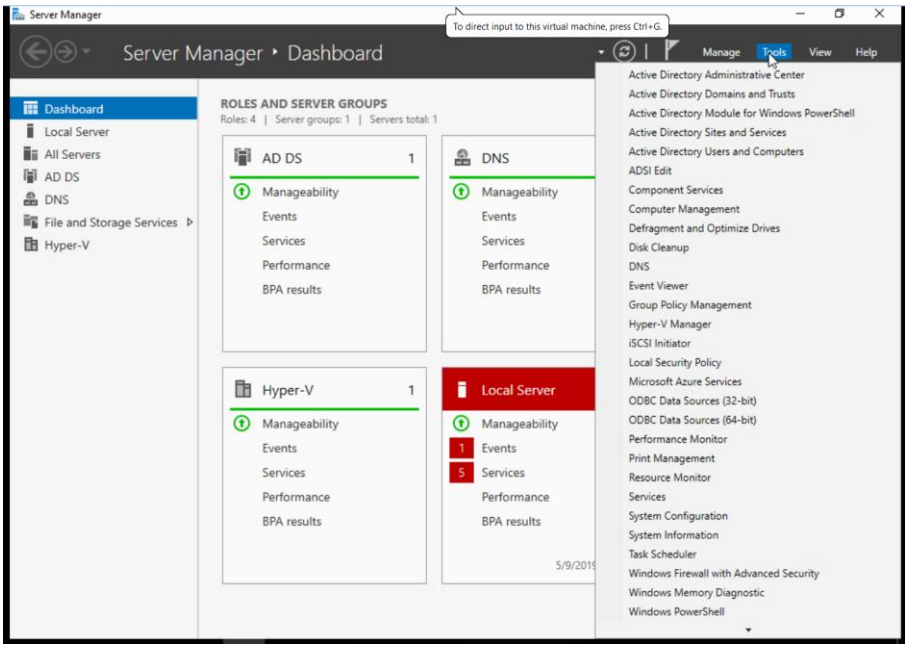

You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close


You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close

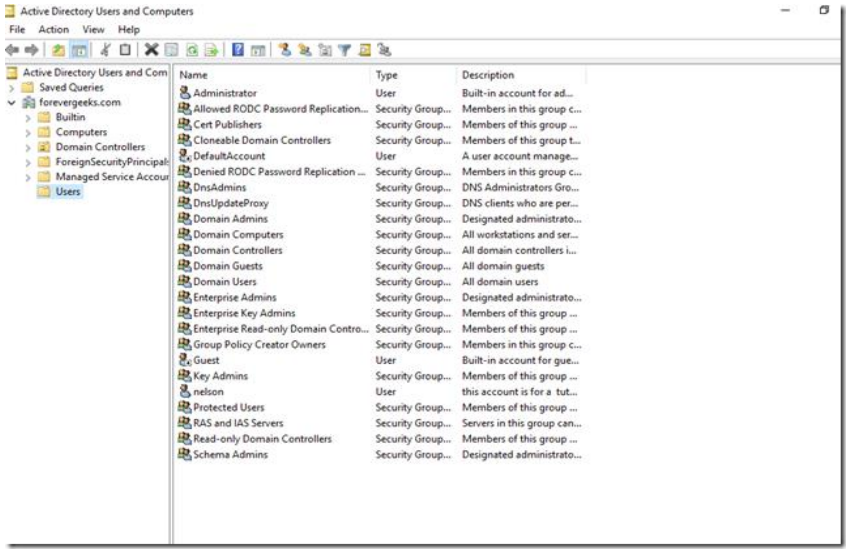

Other user
administrator
Sign in to: FOREVERGEEKS
How do I sign in to another domain?
Other user

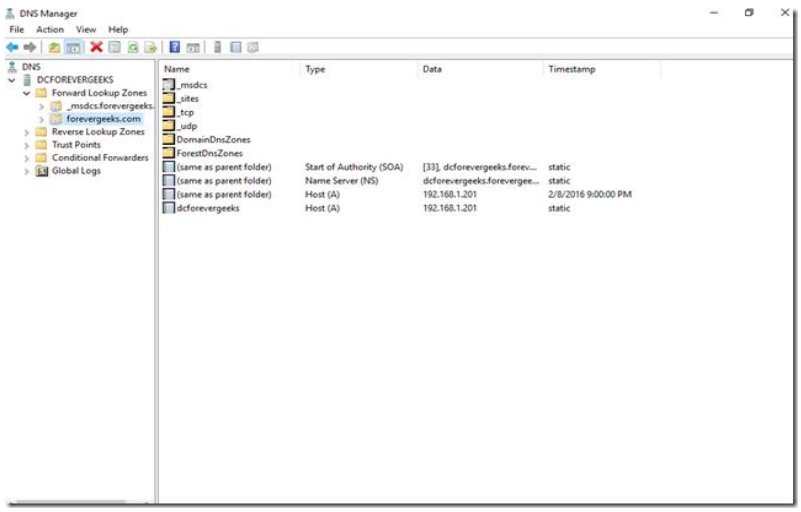
After the installation system will restart automatically. Once it comes back log in to the server as domain admin.

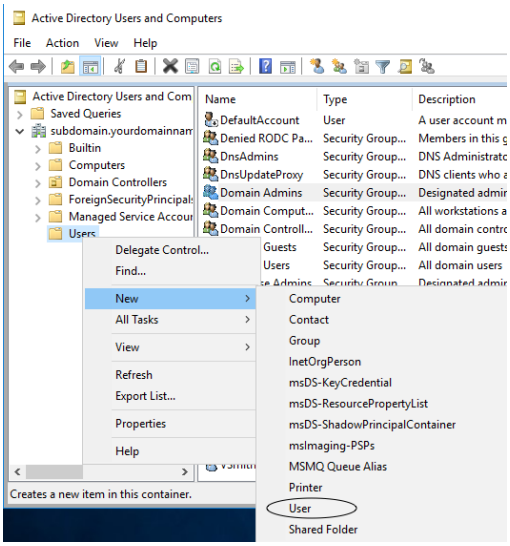


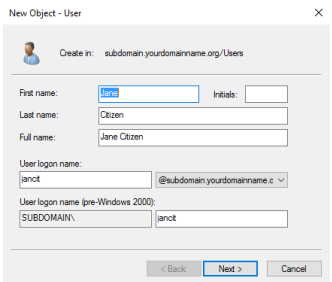


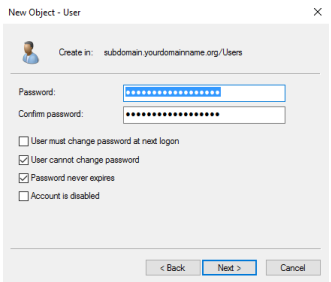
User Account Management

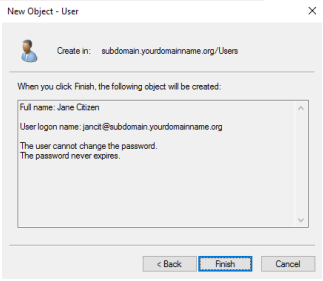


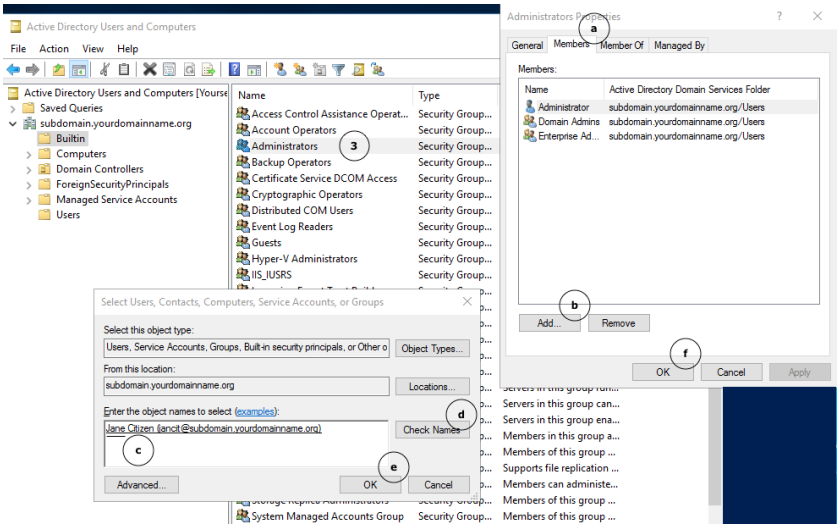


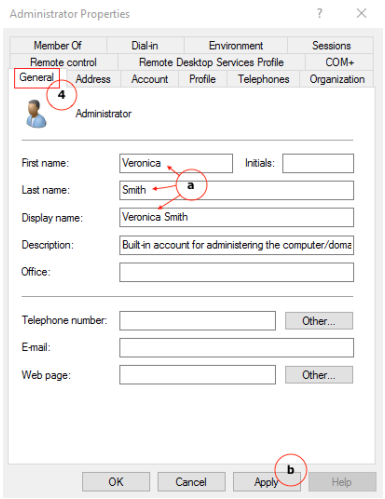

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
subdomain.yourdomainnam
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
Name
Type
Description
DefaultAccount
User
A user account m
Denied RODC Pa...
Security Group...
Members in this g
DnsAdmins
Security Group...
DNS Administrato
DnsUpdateProxy
Security Group...
DNS clients who a
Domain Admins
Security Group...
Designated admir
Domain Comput...
Security Group...
All workstations a
Domain Controll...
Security Group...
All domain contro
Guests
Security Group...
All domain guest
Users
Security Group...
All domain users
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Creates a new item in this container.

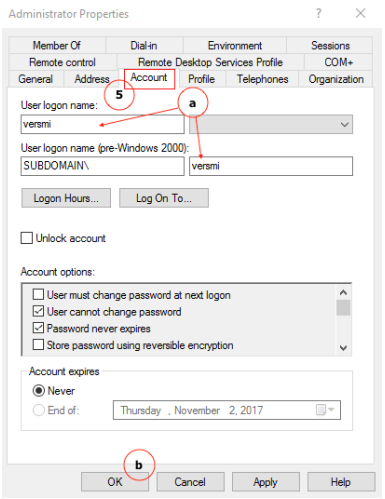

New Object - User
Create in: subdomain.yourdomainname.org/Users
First name:
Initials:
Last name:
Citizen
Full name:
Jane Citizen
User logon name:
jancit
@subdomain.yourdomainname.c
User logon name (pre-Windows 2000):
SUBDOMAIN\
jancit
< Back
Next >
Cancel

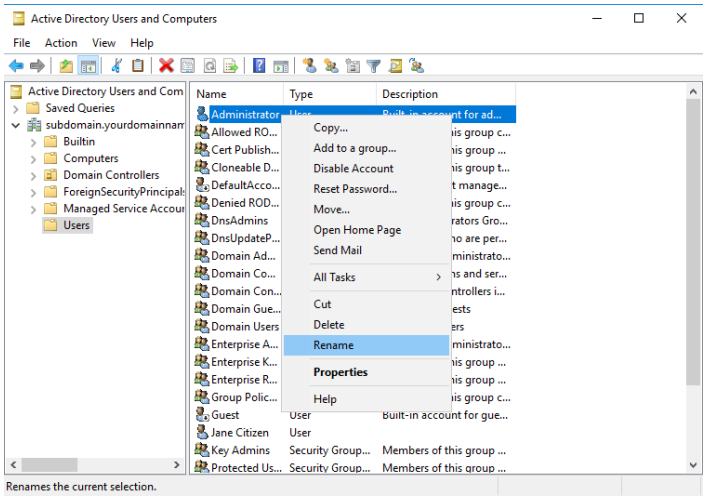

New Object - User
Create in: subdomain.yourdomainname.org/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel

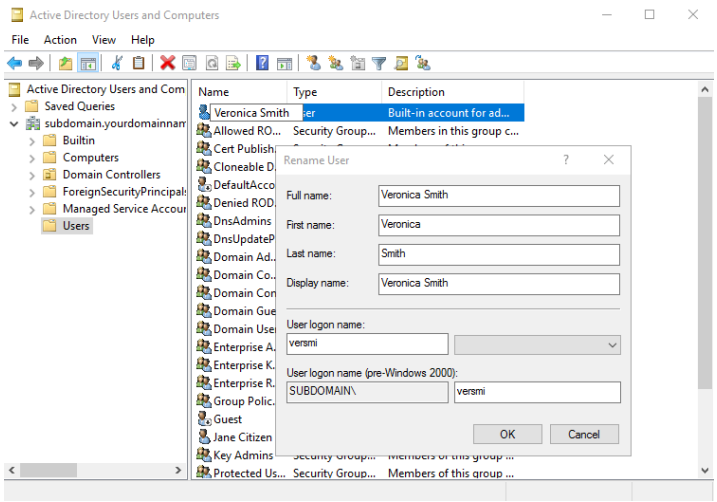

New Object - User
Create in: subdomain.yourdomainname.org/Users
When you click Finish, the following object will be created:
Full name: Jane Citizen
User logon name: jancit@subdomain.yourdomainname.org
The user cannot change the password.
The password never expires.
< Back
Finish
Cancel


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [Yourse
Saved Queries
subdomain.yourdomainname.org
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Access Control Assistance Operat...
Account Operators
Administrators
Backup Operators
Certificate Service DCOM Access
Cryptographic Operators
Distributed COM Users
Event Log Readers
Guests
Hyper-V Administrators
IIS_IUSRS
System Managed Accounts Group
Security Group...
3
Administrators Properties
a
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Administrator
Domain Admins
Enterprise Ad...
subdomain.yourdomainname.org/Users
b
Add...
Remove
f
OK
Cancel
Apply
Select Users, Contacts, Computers, Service Accounts, or Groups
Select this object type:
Users, Service Accounts, Groups, Built-in security principals, or Other o
Object Types...
From this location:
subdomain.yourdomainname.org
Locations...
Enter the object names to select (examples):
Jane Citizen (jancit@subdomain.yourdomainname.org)
Check Names
d
c
e
Advanced...
OK
Cancel


Administrator Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
4
Administrator
First name:
Veronica
Initials:
Last name:
Smith
a
Display name:
Veronica Smith
Description:
Built-in account for administering the computer/dome
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
b
OK
Cancel
Apply
Help

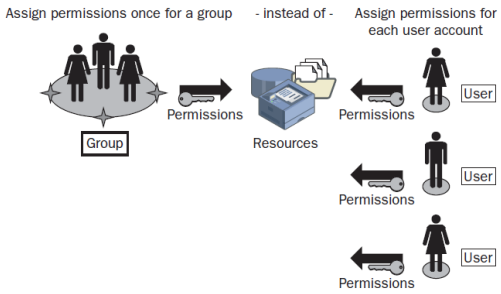

Administrator Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
5
User logon name:
versmi
a
User logon name (pre-Windows 2000):
SUBDOMAIN\
versmi
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Thursday , November 2, 2017
b
OK
Cancel
Apply
Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
subdomain.yourdomainnam
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Administrator
Allowed RO...
Cert Publish...
Cloneable D...
DefaultAcco...
Denied ROD...
DnsAdmins
DnsUpdateP...
Domain Ad...
Domain Co...
Domain Con...
Domain Gue...
Domain Users
Enterprise A...
Enterprise K...
Enterprise R...
Group Polic...
Guest User Built-in account for gue...
Jane Citizen User
Key Admins Security Group... Members of this group ...
Protected Us... Security Group... Members of this group ...
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
Renames the current selection.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
subdomain.yourdomainnam
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Veronica Smith Built-in account for ad...
Allowed RO... Security Group... Members in this group c...
Guest
Jane Citizen
Key Admins
Protected Us... Security Group... Members of this group ...
Rename User
Full name: Veronica Smith
First name: Veronica
Last name: Smith
Display name: Veronica Smith
User logon name:
versmi
User logon name (pre-Windows 2000):
SUBDOMAIN\
versmi
OK
Cancel

ADDS - Groups

- A group is a collection of user accounts. Groups simplify administration by allowing you to assign permissions and rights to a group of users rather than having to assign permissions to each individual user account.



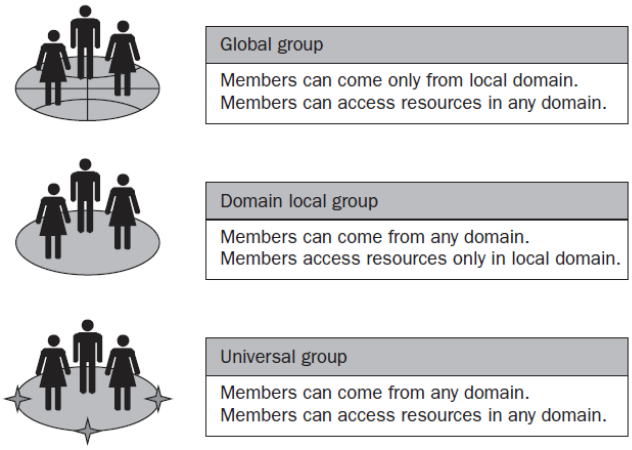
ADDS - Groups

- You can create groups for security-related purposes, such as assigning permissions, or for non-security purposes, such as sending e-mail messages.
- To facilitate this, Active Directory service provides two group types: *security* and *distribution*.
- *Security Groups -Windows Server uses only security groups, which you use to assign permissions to gain access to resources.*

ADDS - Groups

- Distribution Groups - Applications use *distribution groups* as lists for non-security related functions, such as sending e-mail messages to a group of users at the same time.
- You cannot use distribution groups to assign permissions.

ADDS - Groups



Group scopes

ADDS - Groups

Global Groups

Global security groups are most often used to organize users who share similar network access requirements. A global group has the following characteristics:

- **Limited membership** You can add members only from the domain in which you create the global group.
- **Access to resources in any domain** You can use a global group to assign permissions to gain access to resources that are located in any domain in the tree or forest.

ADDS - Groups

Domain Local Groups

Domain local security groups are most often used to assign permissions to resources. A domain local group has the following characteristics:

- **Open membership** You can add members from any domain.
- **Access to resources in one domain** You can use a domain local group to assign permissions to gain access to resources that are located only in the same domain where you create the domain local group.

ADDS - Groups

Universal Groups

The universal group is a new feature beginning in Microsoft Windows 2000. *Universal security groups* are most often used to assign permissions to related resources in multiple domains. A universal security group has the following characteristics:

- **Open membership** You can add members from any domain in the forest.
- **Access to resources in any domain** You can use a universal group to assign permissions to gain access to resources that are located in any domain in the forest.

ADDS - Groups

Global	User accounts and computer accounts from the same domain	User accounts, computer accounts, and global groups from the same domain
Domain local	User accounts, computer accounts, and global groups from any domain	User accounts, computer accounts, global groups, and universal groups from any domain; domain local groups from the same domain
Universal	Not available in domains with a domain functional level set to Windows 2000 mixed	User accounts, computer accounts, global groups, and other universal groups from any domain in the forest

Default Groups in the Builtin

Group Name	Description
Account Operators	This group exists only on domain controllers. By default, the group has no members. By default, members can create, modify, and delete accounts for users, groups, and computers in all containers and OUs of Active Directory except the Builtin folder and the Domain Controllers OU. Members do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.
Administrators	Members have complete and unrestricted access to the computer or domain controller, including the right to change their own permissions. If the Administrator account resides on the first domain controller configured for the domain, the Administrator account is automatically added to the Domain Admins group and complete access to the domain is granted.
Backup Operators	By default, this group has no members. Members can back up and restore all files on a computer, regardless of the permissions that protect those files. Members can also log on to the computer and shut it down.

Default Groups in the Builtin

Print Operators	This group exists only on domain controllers. Members can manage printers and document queues.
Remote Desktop Users	Members can log on to a computer from a remote location.
Replicator	This group supports directory replication functions and is used by the file replication service on domain controllers. By default, the group has no members. The only member should be a domain user account used to log on to the Replicator services of the domain controller. Do not add users to this group.
Server Operators	This group exists only on domain controllers. By default, the group has no members. Members can log on to a server interactively, create and delete network shares, start and stop services, back up and restore files, format the hard disk of the computer, and shut down the computer.

•ADDS management commands

- **Dsquery** * Finds any object in Active Directory by using a generic LDAP query
- **Dsquery computer** Finds computers in the directory
- **Dsquery contact** Finds contacts in the directory
- **Dsquery subnet** Finds subnets in the directory
- **Dsquery group** Finds groups in the directory
- **Dsquery ou** Finds OUs in the directory
- **Dsquery partition** Finds partition objects in the directory
- **Dsquery quota** Finds quota specifications in the directory
- **Dsquery site** Finds sites in the directory
- **Dsquery server** Finds servers in the directory
- **Dsquery user** Finds users in the directory

- To find all computers that have been inactive for the last four weeks, type:

  dsquery computer -inactive 4
- To find all users in the Marketing OU in the domain *microsoft.com*, type:

  dsquery user OU=Marketing,DC=Microsoft,DC=Com
- To find all users with names starting with "Mike," type:

  dsquery user -name Mike*
- To read all attributes of the object whose distinguished name is OU=Test,DC=Microsoft,DC=Com, type:

  dsquery * OU=Test,DC=Microsoft,DC=Com -scope base -attr *

- Csvde, Dsadd, Dsget, Dsmod, Dsmove, Dsquery, Dsrm, Ldifde, and Ntdsutil
- **dsadd ou OU=newOUname,OU=parentOU,DC=domain,DC=com**.

- Distinguished Name
- Every object in Active Directory has a *distinguished name (DN)* that uniquely identifies the object and contains sufficient information
- CN=Scott Cooper,OU=Promotions,OU=Marketing,DC=Microsoft,DC=Com

Tool	Description
DSAdd	Creates an object in the directory
DSGet	Return specified attributes of an object
DSMod	Modifies specified attributes of an object
DSRM	Removes an object and all sub trees
DSQuery	Performs Active Directory query

- **DSADD** Adds objects to the directory.
- **DSGET** Displays ("gets") properties of objects in the directory.
- **DSMOD** Modifies select attributes of an existing object in the directory.
- **DSMOVE** Moves an object from its current container to a new location.
- **DSRM** Removes an object, the complete subtree under an object, or both.
- **DSQUERY** Queries Active Directory for objects that match a specified search criteria. This command is often used to create a list of objects, which are then piped to the other command-line tools for management or modification.

```
C:\>DSAdd user "cn=Simth,cn=users,dc=ITFreeTraining,dc=local" -fn John -ln Simth
 -pwd P@ssw0rd -mustchpwd yes
dsadd succeeded:cn=Simth,cn=users,dc=ITFreeTraining,dc=local
```

```
C:\>DSAdd computer "cn=pc1,cn=computers,dc=ITFreeTraining,dc=local"
```

```
C:\>dsadd group "cn=GSales,ou=Users,ou=New York,dc=ITFreeTraining,dc=local" -sco
pe g_
```

```
C:\>dsrm "OU=Testing,dc=ITFreeTraining,dc=local" -subtree_
```

```
C:\>DSGet user "cn=John Doe,ou=Users,ou=New York,dc=ITFreeTraining,dc=local" -fn
 -ln -email
  fn      ln      email
  John    Doe     DoeJ@ITFreeTraining.local
dsget succeeded
```

```
C:\>dsmod user "cn=Simth,cn=users,dc=ITFreeTraining,dc=local" -pwd P@ssw0rd2 -mu
stchpwd yes_
```

```
C:\>dsrm "OU=Testing,dc=ITFreeTraining,dc=local" -subtree -c
Are you sure you wish to delete OU=Testing,dc=ITFreeTraining,dc=local (Y/N)? n_
```

```
C:\>dsquery ou DC=ITFreeTraining,DC=Local
"OU=Domain Controllers,DC=ITFreeTraining,DC=local"
"OU=New York,DC=ITFreeTraining,DC=local"
"OU=Computers,OU=New York,DC=ITFreeTraining,DC=local"
"OU=Users,OU=New York,DC=ITFreeTraining,DC=local"
"OU=Marketing,OU=Users,OU=New York,DC=ITFreeTraining,DC=local"
"OU=Sales,OU=Users,OU=New York,DC=ITFreeTraining,DC=local"
"OU=test,OU=Computers,OU=New York,DC=ITFreeTraining,DC=local"
"OU=London,DC=ITFreeTraining,DC=local"
"OU=Users,OU=London,DC=ITFreeTraining,DC=local"
"OU=Computers,OU=London,DC=ITFreeTraining,DC=local"
"OU=Testing,DC=ITFreeTraining,DC=local"
```

- **dsquery user "OU=Employees, DC=Contoso,DC=Com" -stalepwd 7**
- The command, which finds user objects that have not changed their password in seven days
- **dsquery user "OU=Employees, DC=Contoso,DC=Com" -stalepwd 7 | dsmod user -mustchpwd yes**
- The command used the results of DSQUERY as the input for the DSMOD command. The DSMOD command configured the option “User must change password at next logon” for each object. Confirm your success by examining the Account tab of the affected objects.

Operations master roles - FSMOs

- Operations master roles (also known as flexible single master operations, or FSMO) are special roles assigned to one or more domain controllers in an Active Directory domain.

- The domain controllers assigned these roles perform single-master replication.

Operations master roles - FSMO

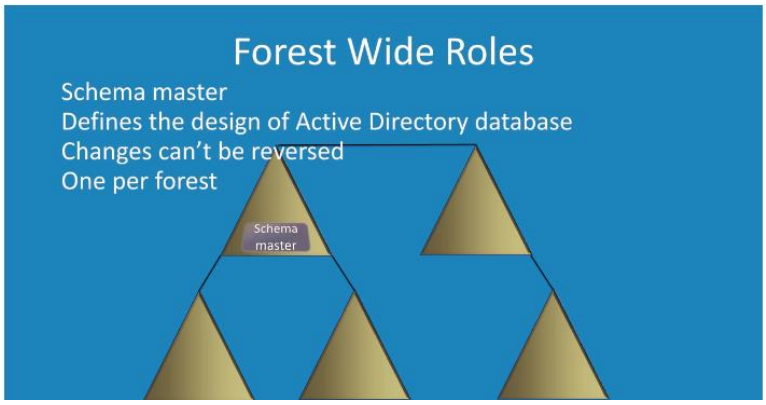
- Active Directory supports multimaster replication of the Active Directory database between all domain controllers in the domain.
- However, some changes are impractical to perform in multimaster fashion, so one or more domain controllers can be assigned to perform operations that are single-master (not permitted to occur at different places in a network at the same time).
- Operations master roles are assigned to domain controllers to perform single-master operations.

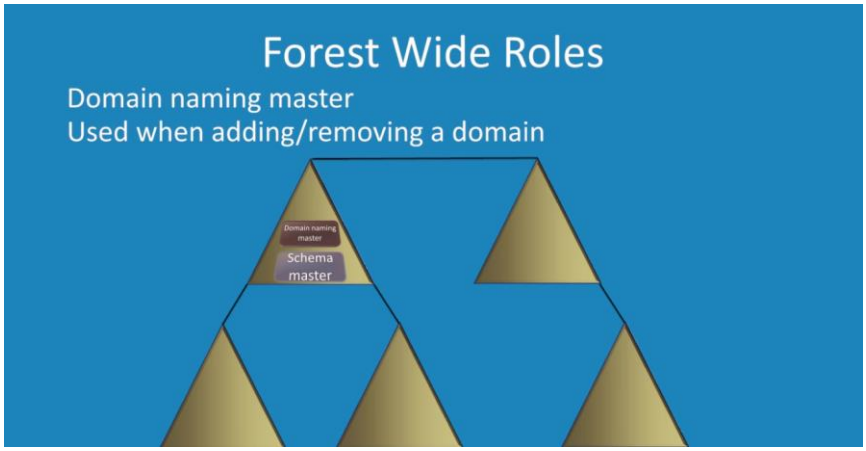
Operations master roles - FSMO

- Forest-Wide Operations Master Roles –
  - Schema master
  - Domain naming master
- Domain-Wide Operations Master Roles - Every domain in the forest must have the following roles:
  - Relative identifier (RID), or relative ID, master
  - Primary domain controller (PDC) emulator
  - Infrastructure master

Operations master roles - FSMO

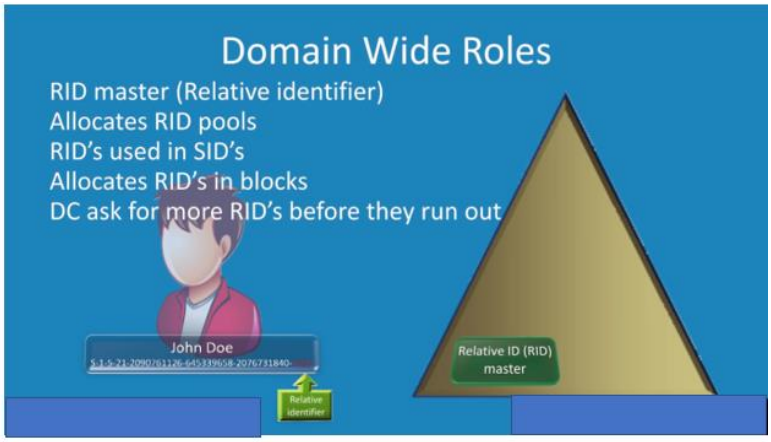
- Schema Master Role
- The domain controller assigned the *schema master* role controls all updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master. At any time, there can be only one schema master in the entire forest.
- Domain Naming Master Role
- The domain controller holding the domain naming master role controls the addition or removal of domains in the forest. There can be only one domain naming master in the entire forest at any time.

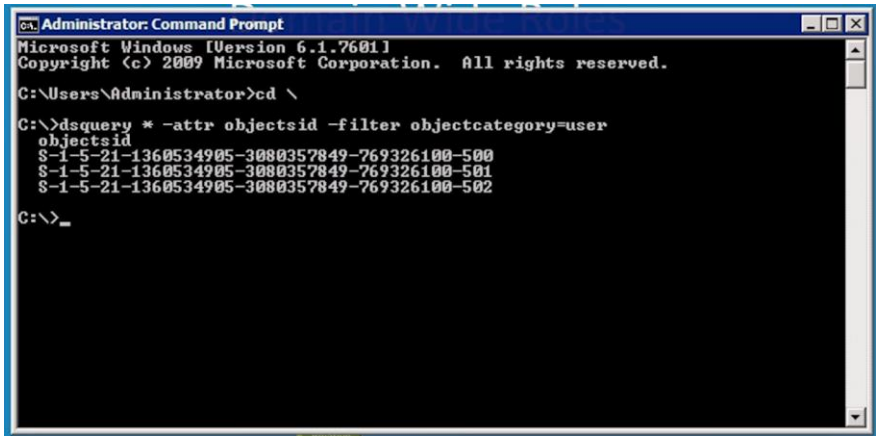




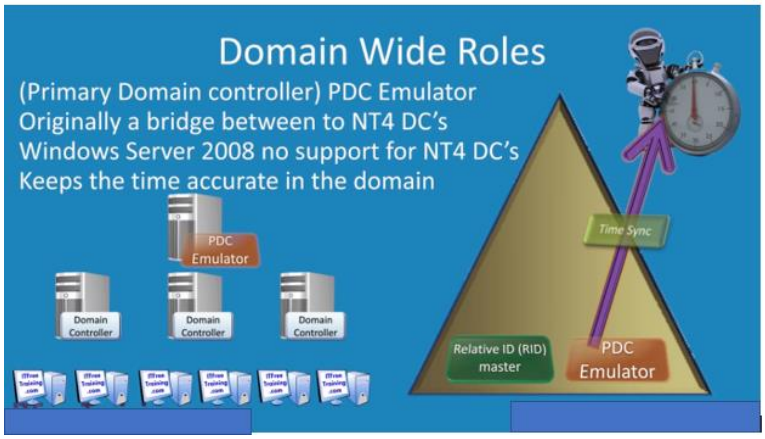
Operations master roles - FSMO

- RID Master Role
- The domain controller assigned the *RID master* role allocates sequences of relative IDs to each of the various domain controllers in its domain. At any time, there can be only one domain controller acting as the RID master in each domain in the forest.
- Whenever a domain controller creates a user, group, or computer object, it assigns the object a unique security ID. The security ID consists of a domain security ID (that is the same for all security IDs created in the domain) and a relative ID that is unique for each security ID created in the domain.
- To move an object between domains (using Movetree.exe: Active Directory Object Manager), you must initiate the move on the domain controller acting as the RID master of the domain that currently contains the object.

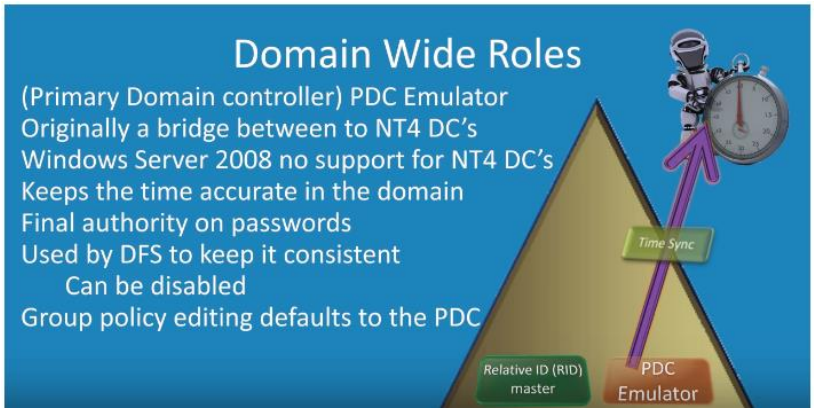

Domain Wide Roles
RID master (Relative identifier)
Allocates RID pools
RID's used in SID's
Allocates RID's in blocks
DC ask for more RID's before they run out
John Doe
Relative identifier
Relative ID (RID) master


Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd \
C:\>dsquery * -attr objectsid -filter objectcategory=user
objectsid
S-1-5-21-1360534905-3080357849-769326100-500
S-1-5-21-1360534905-3080357849-769326100-501
S-1-5-21-1360534905-3080357849-769326100-502
C:\>

PDC Emulator

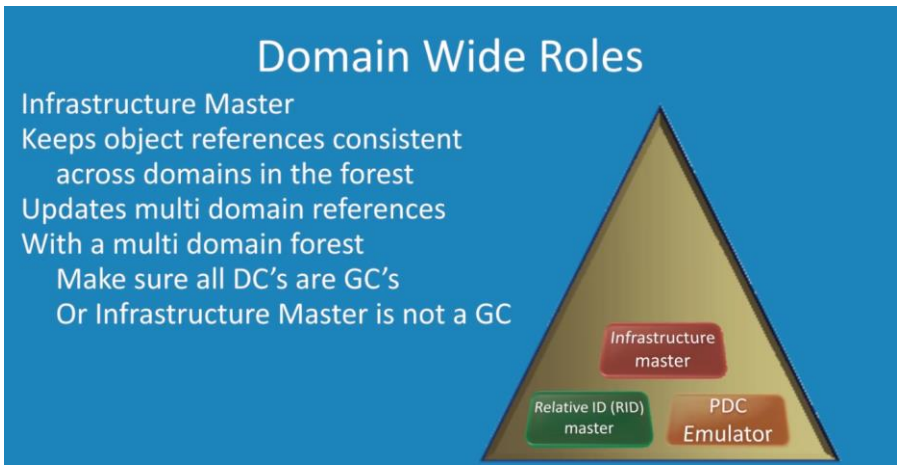


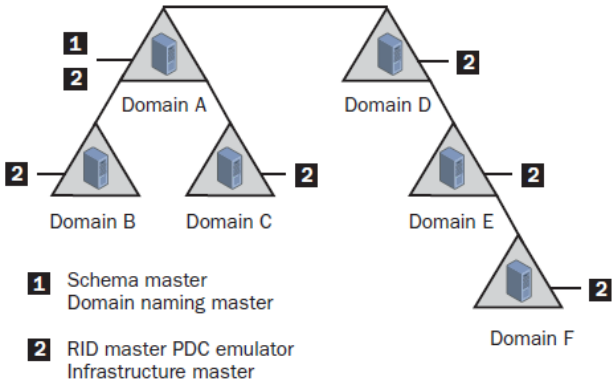
PDC Emulator



Operations master roles - FSMO

- Infrastructure Master Role
- The domain controller assigned the *infrastructure master* role is responsible for updating the group-to-user references whenever the members of groups are renamed or changed. At any time, there can be only one domain controller acting as the infrastructure master in each domain.



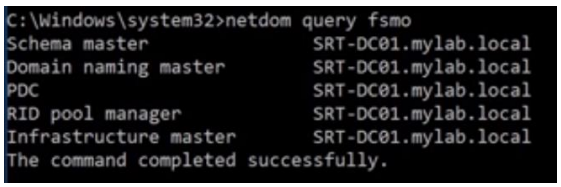


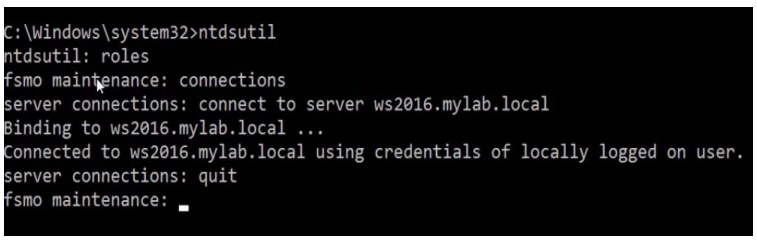
Operations master role default distribution in a forest

Operations Master Roles

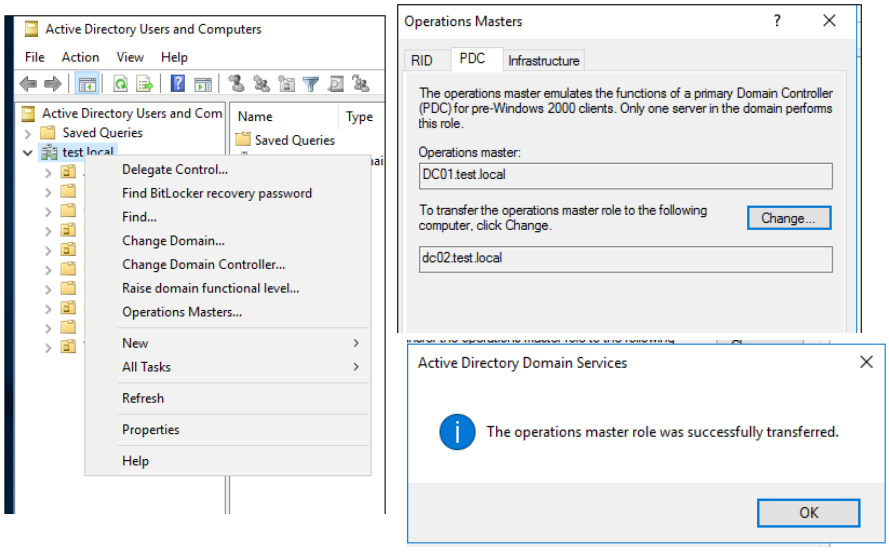
- Transferring Operations Master Roles
- To transfer an operations master role is to move it with the cooperation of its current owner. You transfer an operations master role when you want to move a role from one server to another.
- Seizing Operations Master Roles
- To seize an operations master role is to move it without the cooperation of its current owner. You seize an operations master role assignment when a server that is holding a role fails and you do not intend to restore it.

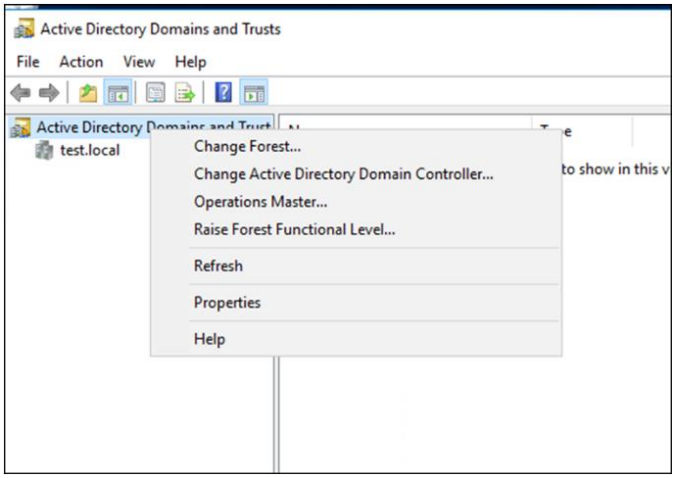
- Before seizing the operations master role, determine the cause and expected duration of the computer or network failure. If the cause is a networking problem or a server failure that will be resolved soon, wait for the role holder to become available again.
- If the domain controller that currently holds the role has failed, you must determine if it can be recovered and brought back online. In general, seizing an operations master role is a drastic step that should be considered only if the current operations master will never be available again.
- The decision depends upon the role and how long the particular role holder will be unavailable. The impact of various role holder failures is discussed in the following topics.

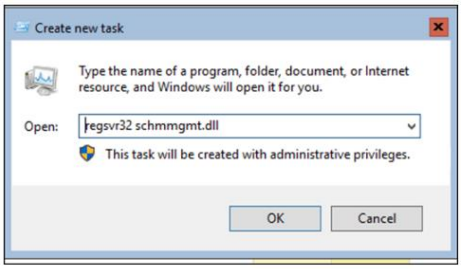


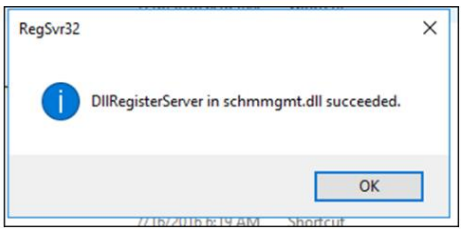


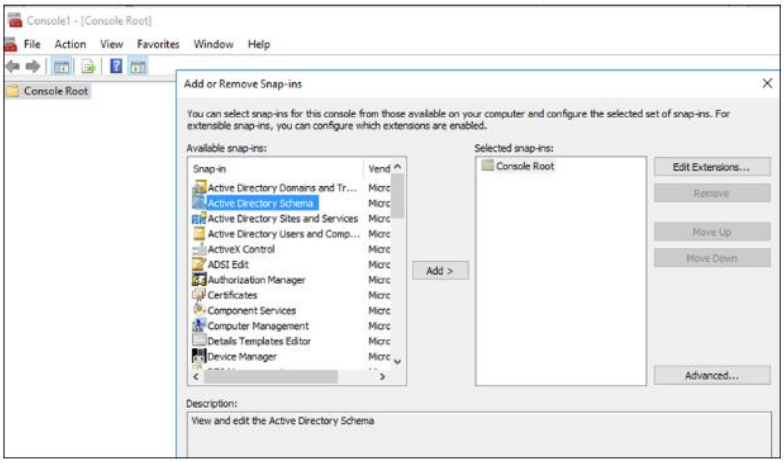
```
fsmo maintenance: ?

?                               - Show this help information
Connections                     - Connect to a specific AD DC/LDS instance
Help                            - Show this help information
Quit                            - Return to the prior menu
Seize infrastructure master     - Overwrite infrastructure role on connected server
Seize naming master             - Overwrite Naming Master role on connected server
Seize PDC                       - Overwrite PDC role on connected server
Seize RID master                - Overwrite RID role on connected server
Seize schema master             - Overwrite schema role on connected server
Select operation target         - Select sites, servers, domains, roles and
                                  naming contexts
Transfer infrastructure master - Make connected server the infrastructure master
Transfer naming master          - Make connected server the naming master
Transfer PDC                    - Make connected server the PDC
Transfer RID master             - Make connected server the RID master
Transfer schema master          - Make connected server the schema master
```

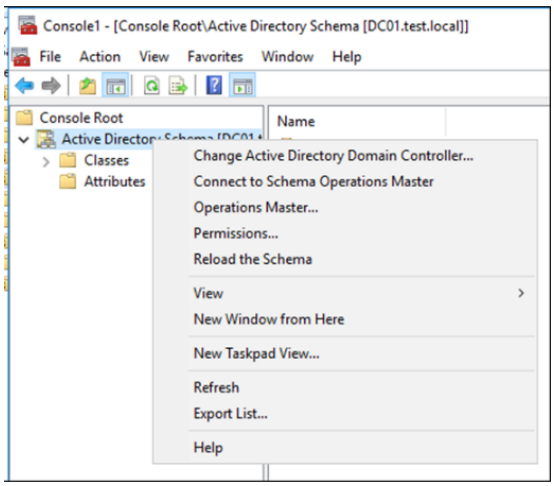



Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
test.local
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
Refresh
Properties
Help


Create new task
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
regsvr32 schmmgmt.dll
This task will be created with administrative privileges.
OK
Cancel


RegSvr32
DllRegisterServer in schmmgmt.dll succeeded.
OK


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vend
Active Directory Domains and Tr...
Active Directory Schema
Active Directory Sites and Services
Active Directory Users and Comp...
ActiveX Control
ADSI Edit
Authorization Manager
Certificates
Component Services
Computer Management
Details Templates Editor
Device Manager
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
View and edit the Active Directory Schema


Console1 - [Console Root\Active Directory Schema [DC01.test.local]]
File Action View Favorites Window Help
Console Root
Active Director
Classes
Attributes
Name
Change Active Directory Domain Controller...
Connect to Schema Operations Master
Operations Master...
Permissions...
Reload the Schema
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

- `DSA.MSC`: Active Directory Users and Computers
- `DSSITE.MSC`: Active Directory Sites and Services
- `DNSMGMT.MSC`: DNS Manager
- `GPEDIT.MSC`: Local Group Policy Editor
- `GPMC.MSC`: Group Policy Management Console
- `CERTSRV.MSC`: Certification Authority Management
- `CERTTMPL.MSC`: Certificate Template Management
- `CERTLM.MSC`: Local Computer Certificates Store
- `COMPMGMT.MSC`: Computer Management
- `DEVMGMT.MSC`: Device Manager
- `DHCPMGMT.MSC`: DHCP Manager
- `DISKMGMT.MSC`: Disk Management
- `EVENTVWR.MSC`: Event Viewer
- `PERFMON.MSC`: Performance Monitor
- `SECPOL.MSC`: Local Security Policy Console
- `FSMGMT.MSC`: Shared Folders
- `WF.MSC`: Windows Firewall with Advanced Security

This is a list of the most common active directory mmc console run commnad that is really usefull in my opinion :

CERTMGR.MSC	Certificates snap-in
CERTSRV.MSC	Certification Services
CMD.EXE	Command Prompt
COMPMGMT.MSC	Computer Management
DCPOL.MSC	Domain Controller Security Policy
DEVMGMT.MSC	Device Manager
DFRG.MSC	Disk Defragmenter
DFSGUI.MSC	Distributed File System
DHCPMGMT.MSC	DHCP Manager
DISKMGMT.MSC	Disk Management
DNSMGMT.MSC	DNS Manager
DOMAIN.MSC	Active Directory Domains & Trust
DOMPOL.MSC	Domain Security Policy
DSA.MSC	Active Directory Users & Computers
DSA.MSC /DOMAIN=domainname	
DSA.MSC /SERVER=servername	
DSSITE.MSC	Active Directory Sites & Services
EVENTVWR.MSC	Event Viewer
FSMGMT.MSC	Shared Folders

EVENTVWR.MSC	Event Viewer
FSMGMT.MSC	Shared Folders
GPEDIT.MSC	local Group Policy Editor
IAS.MSC	Internet Authentication Service
INETMGR	Internet Information Service (\Windows\system32\inetsrv)
LUSRMGR.MSC	Local Users and Groups
MMC.EXE	Microsoft Management Console
MSINFO32.EXE	Hardware and software configuration information
PERFMON.MSC	Performance Monitor
REGEDIT.EXE	Run Registry Editor
RRASMGMT.MSC	Routing and Remote Access
RSOP.MSC	Resultant Set of Policy
SECPOL.MSC	Local Security Policy
SERVICES.MSC	Service Configuration
TSCC.MSC	Terminal Services
MSTSC	Remote Desktop

Active Directory

Item	Command
Active Directory Rights Management Services	AdRmsAdmin.msc
ADSI Edit	adsiedit.msc
Active Directory Certificate Services	certsrv.msc
DFS Management	dfsmgmt.msc
DHCP Console	dhcpmgmt.msc
Disk Management	diskmgmt.msc
DNS Console	dnsmgmt.msc
Active Directory Domains and Trust	domain.msc
Active Directory Users and Computers	dsa.msc
Active Directory Site and Subnets	dssite.msc
Event Viewer	eventvwr.msc
Group Policy Management Console	gpmc.msc
Group Policy Management Editor	gpme.msc
LDP	ldp.exe
PKI - Enterprise PKI	pkiview.msc
Resultant Set of Policy	rsop.msc
Server Manager	ServerManager.msc
WINS	winsmgmt.msc
WMI	WmiMgmt.msc

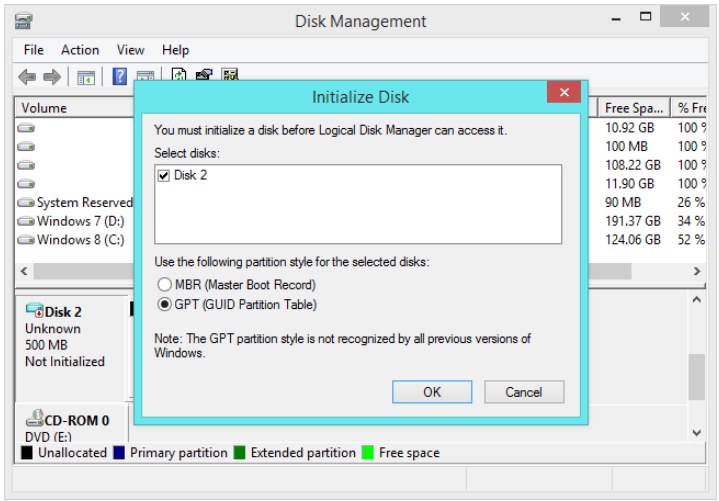
Windows Server

Item	Command
Active Directory Rights Management Services	AdRmsAdmin.msc
ADSI Edit	adsiedit.msc
Authorization Manager	azman.msc
Certificates	certmgr.msc
Active Directory Certificate Services	certsrv.msc
Certificate Templates Console	certtmpl.msc
Cluster Admin	CluAdmin.msc
Component Services	comexp.msc
Computer Manager	compmgmt.msc
Device Manager	devmgmt.msc
DFS Management	dfsmgmt.msc
DHCP Console	dhcpmgmt.msc
Disk Management	diskmgmt.msc
DNS Console	dnsmgmt.msc
Active Directory Domains and Trust	domain.msc
Active Directory Users and Computers	dsa.msc
Active Directory Site and Subnets	dssite.msc
Event Viewer	eventvwr.msc
Failover Cluster Manager	FailoverClusters.SnapInHelper.msc
Shared Folders Console	fsmgmt.msc
File Server Resource Manager	fsrm.msc
Fax Service Manager	fxsadmin.msc
Local Group Policy Editor	gpedit.msc
Group Policy Management Console	gpmc.msc
Group Policy Management Editor	gpme.msc
GPO Editor	gptedit.msc
Local Users and Groups	lusrmgr.msc
NAP Client Configuration	NAPCLCFG.MSC
Services for Network File System	nfsmgmt.msc
Performance Monitor	perfmon.msc
PKI - Enterprise PKI	pkiview.msc
Print Management	printmanagement.msc
Remote App Manager	remoteprograms.msc
Resultant Set of Policy	rsop.msc
Remote Desktop Connection Manager	sbmgr.msc
Local Security Policy	secpol.msc
Server Manager	ServerManager.msc
Services	services.msc
SQL Server Configuration Manager	SQLServerManager10.msc
Share and Storage Management	StorageMgmt.msc
Storage Explorer	StorExpl.msc
Telephony	tapimgmt.msc
Task Scheduler	taskschd.msc
TPM Management Console	tpm.msc
Remote Desktop Services Manager	tsadmin.msc
Remote Desktops Session Host Configuration	tsconfig.msc
RD Gateway Manager	tsgateway.msc
Remote Desktops - Console Root\Remote Desktops	tsmmc.msc
Windows Server Backup	wbadmin.msc
Windows Deployment Services	WdsMgmt.msc
Windows Firewall and Advanced Security	WF.msc
WINS	winsmgmt.msc
WMI	WmiMgmt.msc

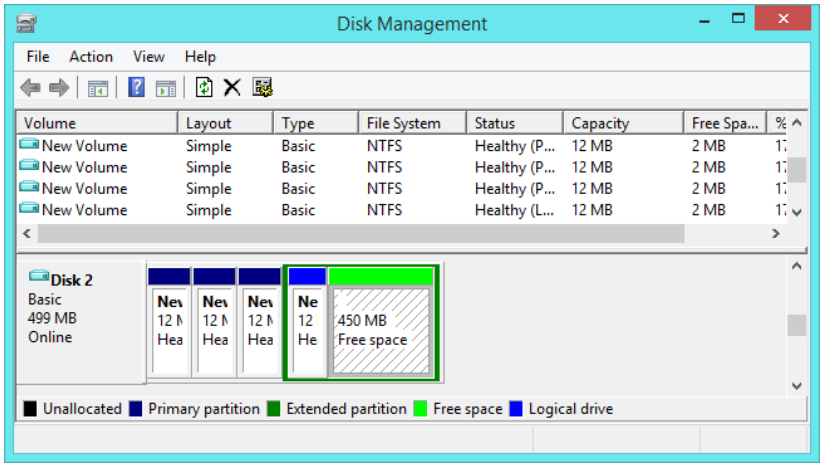
Overview of Storage

- Primary Memory
- Secondary Memory (Auxiliary Memory)
- Storage Devices – PATA(IDE), SATA, SSD

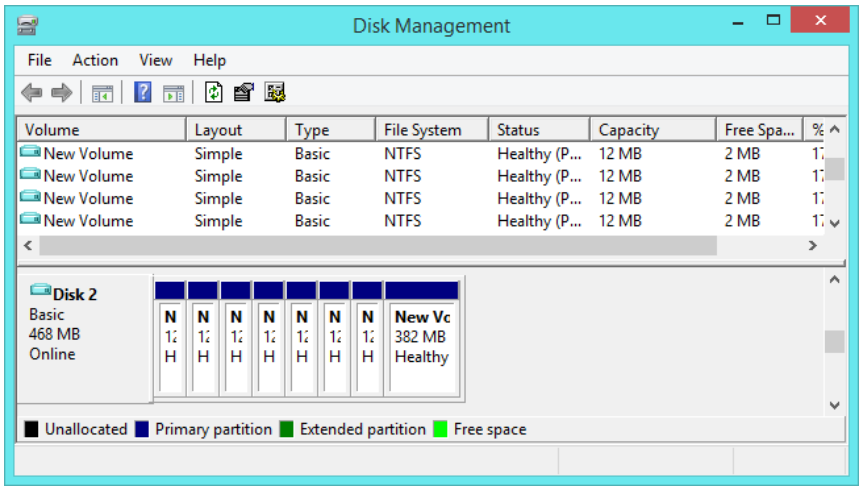
Managing Disks and Volumes



Disk Management



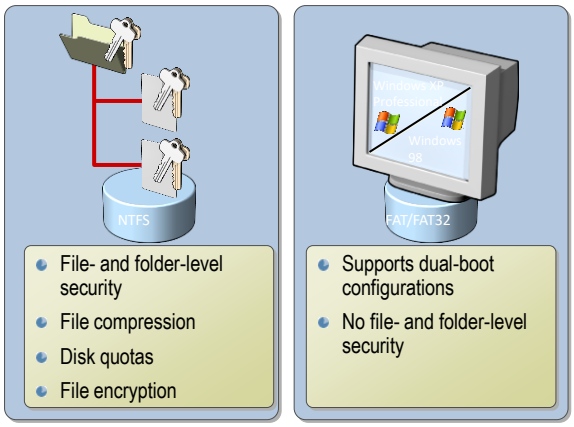
Disk Management



Securing Files and Folders

Configuring and managing file access
Securing Files and Folders

Security Permissions(NTFS)



Choosing the Appropriate File System: FAT, FAT32, or the NTFS File System

Security Permissions(NTFS)

NTFS Premissions

Applied to a file or folder to allow or deny access

NTFS Standard Permissions	
List folder content	Allows the file in a folder to be displayed
Read	Allows the file or folder to read
Read & Execute	Allows reading and application execution
Write	Write but can't delete any files
Modify	Can read, write and delete. The most common permissions assigned to end user
Full control	All of the above plus changing permissions, owner.

Configuring and managing file access

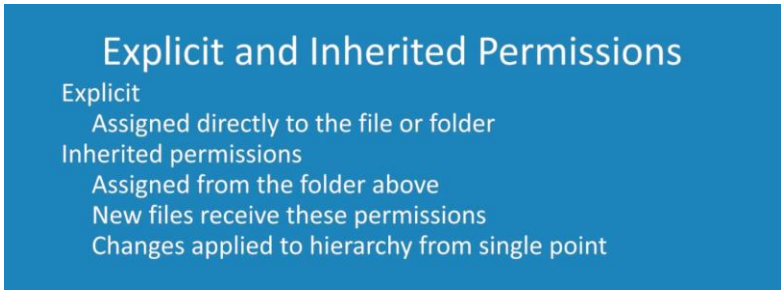
Allow & Deny

Allows permissions are accumulatively
Deny override all other permissions

Copying and moving files

Moving to same volume permissions are retained
All other combinations permissions are inherited

Configuring and managing file access



Work Folders

- In Server Manager, click File and Storage Services, and then click Servers. Right-click the sync server, and then click **Work Folders Settings**. The **Work Folders Settings** window appears.
- With Work Folders users can store and access work files on personal computers and devices, often referred to as bring-your-own device (BYOD), in addition to corporate PCs. Users gain a convenient location to store work files, and they can access them from anywhere.

Work Folders – Offline Files

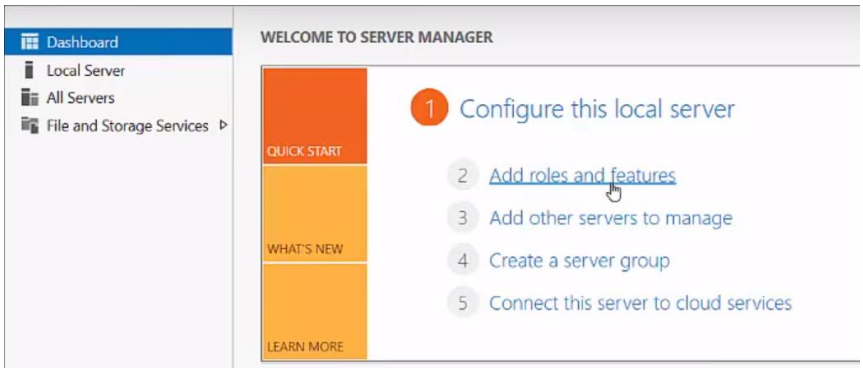
- Organizations maintain control over corporate data by storing the files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.

- Work Folders can be deployed with existing deployments of Folder Redirection, Offline Files, and home folders. Work Folders stores user files in a folder on the server called a sync share. You can specify a folder that already contains user data, which enables you to adopt Work Folders without migrating servers and data or immediately phasing out your existing solution.

Work Folders

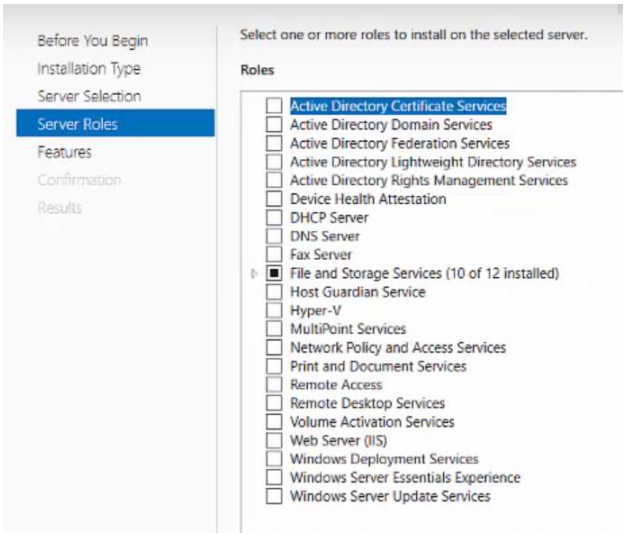
- Organizations maintain control over corporate data by storing the files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.
- Work Folders can be deployed with existing deployments of Folder Redirection, Offline Files, and home folders. Work Folders stores user files in a folder on the server called a *sync share*.
- You can specify a folder that already contains user data, which enables you to adopt Work Folders without migrating servers and data or immediately phasing out your existing solution.

Work Folders

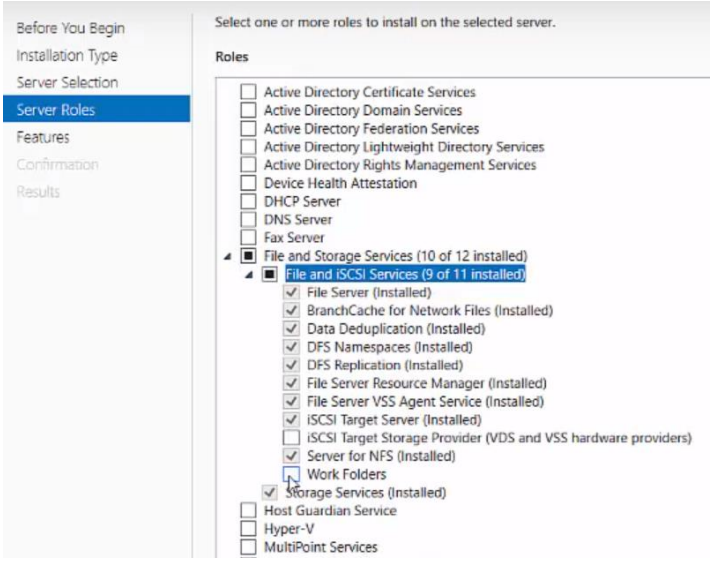


Work Folders

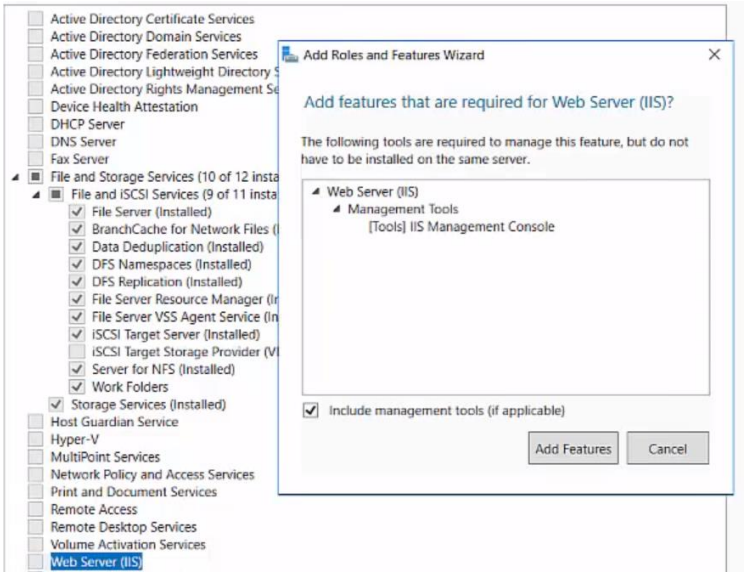
Work Folders



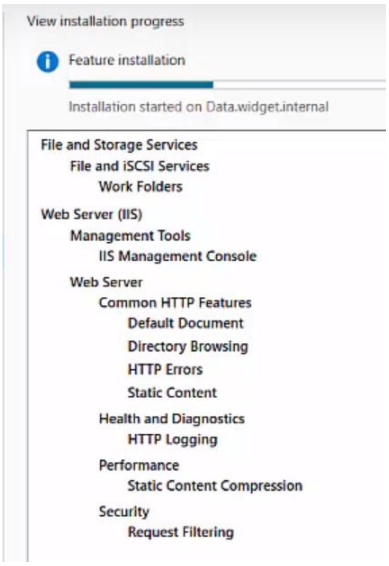
Work Folders



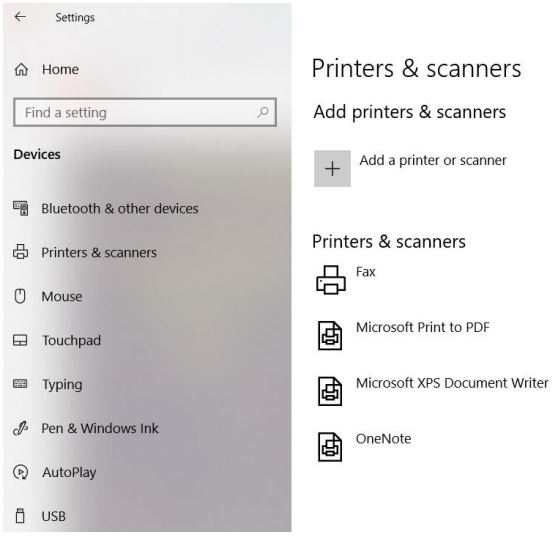
Work Folders



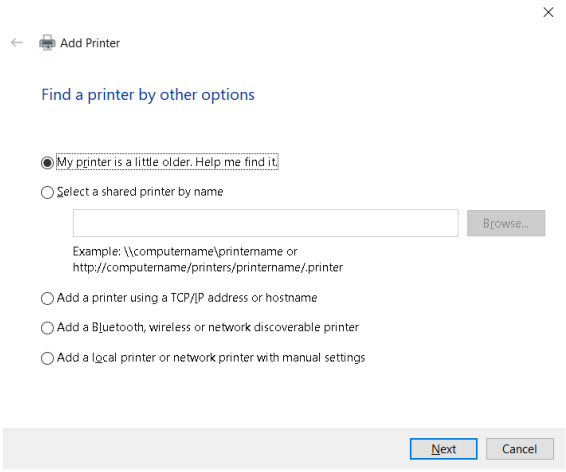
Work Folders



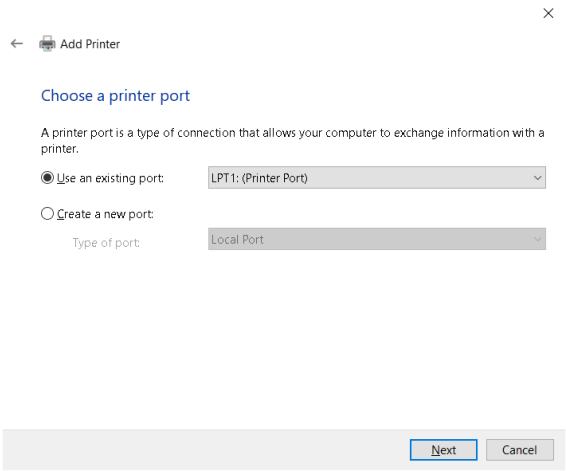
Printer Management



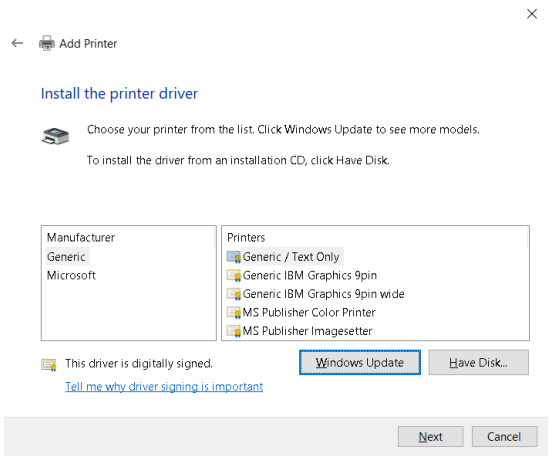
Printer Management



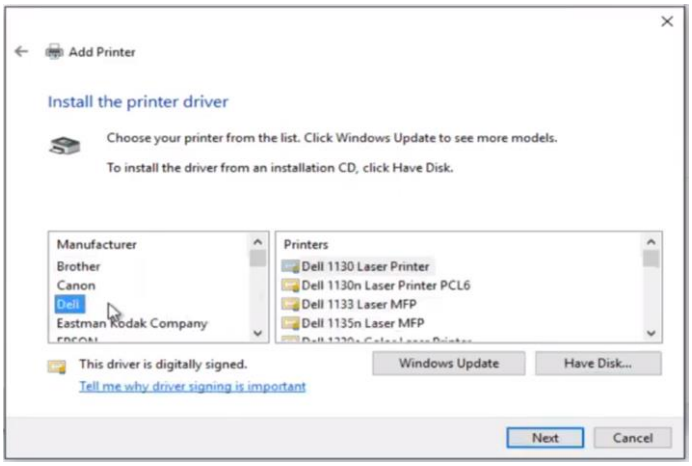
Printer Management



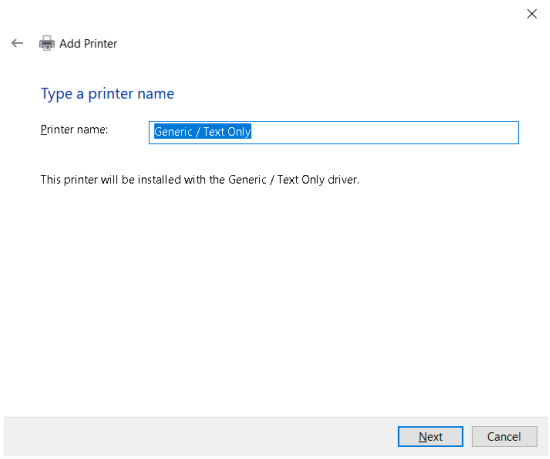
Printer Management



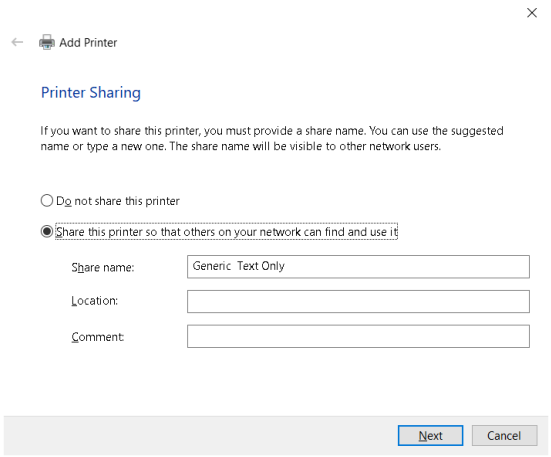
Printer Management



Printer Management



Printer Management



Printer Management