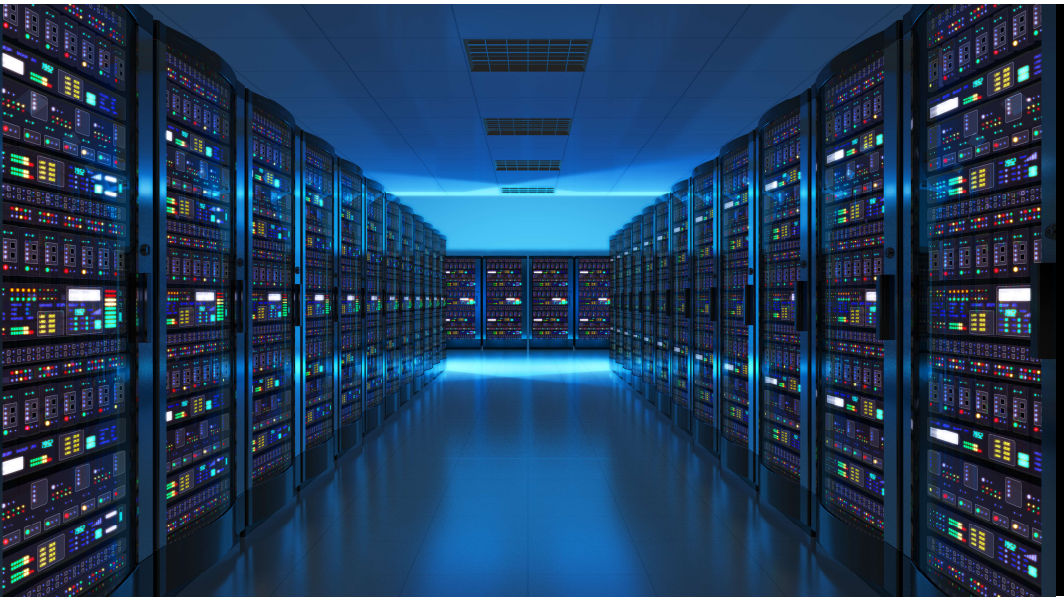


Windows Server 2022 Administration

Kevin Brown
MCT (Microsoft Certified Trainer) since 2000
Azure Security Engineer
Azure Solutions Architect
Azure Administrator
Microsoft 365 Enterprise Administrator
MCSE NT 4.0, 2000, 2003, 2008, 2012, 2016
CISSP

What you will learn

Server 2022

Active Directory

Domain

Bonus

VPN Remote Access

SAN

Virtual Machines

File Servers

DHCP
DNS
WSUS
Failover Clustering
Disaster Recovery

Course Outline

1. Introduction to Windows Server 2022
2. Active Directory Domain Services on Windows Server 2022
3. Managing DHCP on Windows Server 2022
4. Managing DNS on Windows Server 2022
5. Implementing File Servers and Storage
6. Implementing Hyper-V Virtualization
7. Implementing Windows Print Servers on Windows Server 2022
8. Disaster Recovery in Windows Server 2022
9. Managing SAN Storage and Failover Clustering
10. Implementing WSUS on Windows Server 2022
11. Implementing Remote Access on Windows Server 2022
12. Performance Monitoring in Windows Server 2022

Microsoft Azure

Windows Server 2022 integration with Azure Virtual Machines

Windows Server 2022 integration with Azure File Shares

Windows Server 2022 integration with Microsoft Entra ID (formerly Azure AD)

Lab Setup

Hyper-V lab

Windows Server 2022 ISO download

Enabling Hyper-V

Installing Windows Server 2022 using Hyper-V

Hyper-V post installation tasks

VirtualBox lab

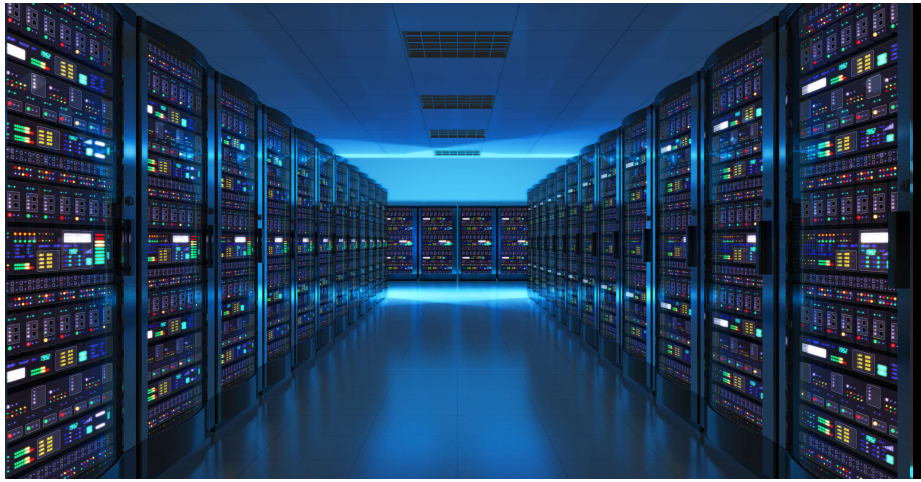
Windows Server 2022 ISO download

Installing VirtualBox

Installing Windows Server 2022 using VirtualBox

VirtualBox post installation tasks

https://rtsnetworking.com/demo



Module 1:

Introducing Windows Server 2022

Module overview

This module introduces you to Windows Server 2022

Lessons

- Requirements for Windows Server 2022
- Windows Server 2022 Editions
- Deployment Options
- Overview of Windows Server Core
- Overview of administration methods and tools

Lesson 1 overview

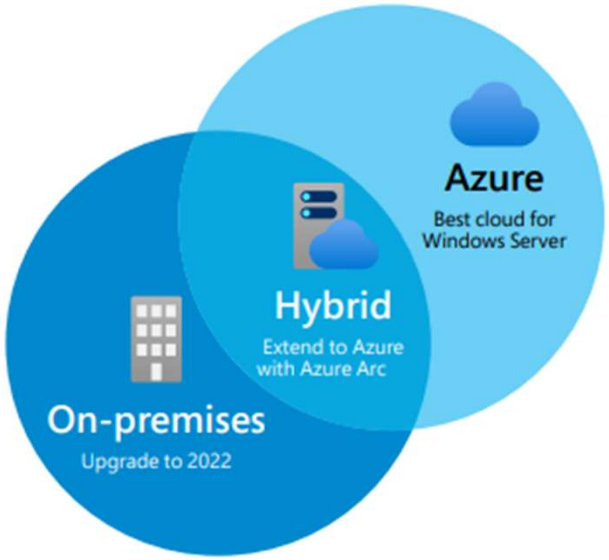
In this lesson, you'll learn about Windows Server 2022 editions and their capabilities

- Topics
  - Windows Server 2022 editions
  - Hardware requirements for Windows Server 2022
  - Overview of deployment options
  - Servicing channels for Windows Server
  - Licensing and activation for Windows Server

Windows Server 2022 editions

Windows Server 2022 is released in four editions:

- Windows Server 2022 Essential
  - Small businesses with up to 25 users and 50 devices
- Windows Server 2022 Standard
  - Physical or minimally virtualized environments
- Windows Server 2022 Datacenter
  - Highly virtualized datacenters
- Windows Server 2022 Azure edition:
  - Allows you to run Server 2022 as a VM in Azure.

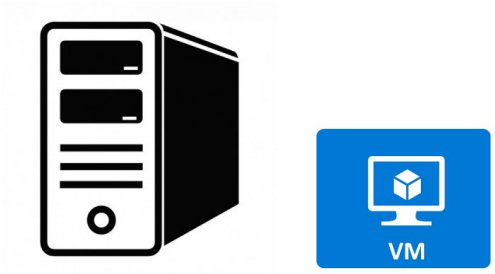


Edition Comparison

- https://learn.microsoft.com/windows-server/get-started/editions-comparison-windows-server-2022?tabs=full-comparison

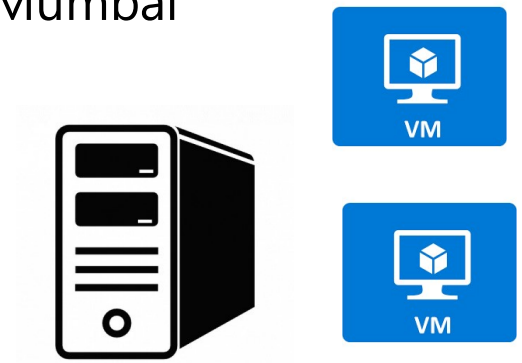
Windows Server 2022 editions

Kuala Lumpur



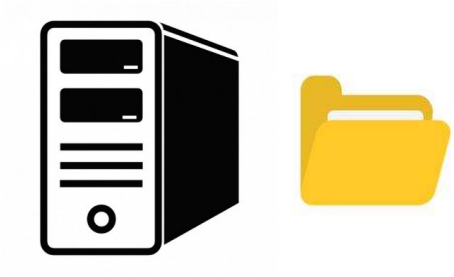
Standard

Mumbai



Datacenter

Sydney



Standard

Windows Server 2022 Azure Edition

Azure Automanage - Hotpatch

Hotpatching, part of Azure Automanage, is a new way to install updates on new Windows Server Azure Edition virtual machines (VMs) that doesn't require a reboot after installation.

SMB over QUIC (Quick UDP Internet Connection)

SMB over QUIC updates the SMB 3.1.1 protocol to use the QUIC protocol instead of TCP in Windows Server 2022 Datacenter: Azure Edition, Windows 11 and later, and third party clients if they support it. By using SMB over QUIC along with TLS 1.3, users and applications can securely and reliably access data from edge file servers running in Azure. Mobile and telecommuter users no longer need a VPN to access their file servers over SMB when on Windows.

Extended network for Azure

Azure Extended Network enables you to stretch an on-premises subnet into Azure to let on-premises virtual machines keep their original on-premises private IP addresses when migrating to Azure.

About Microsoft Azure

The bonus module of this course will cover Azure topics:

- Creating an Azure subscription
- Creating Azure Virtual Machines
- Creating Azure Storage Accounts
- Creating Azure File Shares
- Understanding Microsoft Entra ID (formerly Azure AD)
- Creating and managing Entra ID users and groups
- Synchronizing on-premises Active Directory Domain Services to Microsoft Entra ID in Azure

Windows Server 2022 editions

Edition removed: Hyper-V server 2019 is that products last version and will continue to be supported under its lifecycle policy until January 2029

End-of-Life Support for Windows Server 2022

Listing	Start Date	Mainstream End Date	Extended End Date
Windows Server 2022	Aug 18, 2021	Oct 13, 2026	Oct 14, 2031

Listing	Start Date	Mainstream End Date	Extended End Date
Windows Server 2022	August 18, 2021	October 13, 2026	October 14, 2031
Windows Server 2019	November 13, 2018	January 9, 2024	January 9, 2029
Windows Server 2016	October 10, 2015	End of Servicing	January 11, 2027
Windows Server 2012R2	November 25, 2013	End of Servicing	October 10, 2023

Windows Server 2012R2 offers Extended Security Updates through October 13, 2026.

Windows **mainstream** and **extended** end dates refer to the support life cycle for each new version of Windows. **Mainstream support** lasts for **five years** and **includes non-security hotfixes, and new features**. **Extended support** lasts for **another five years and only includes security and reliability patches**. After extended support ends, the version of Windows is no longer supported by Microsoft.

Hardware requirements for Windows Server 2022

- Hardware requirements will vary depending on:
  - Server roles
    - Many roles have specific requirements
  - Resource usage

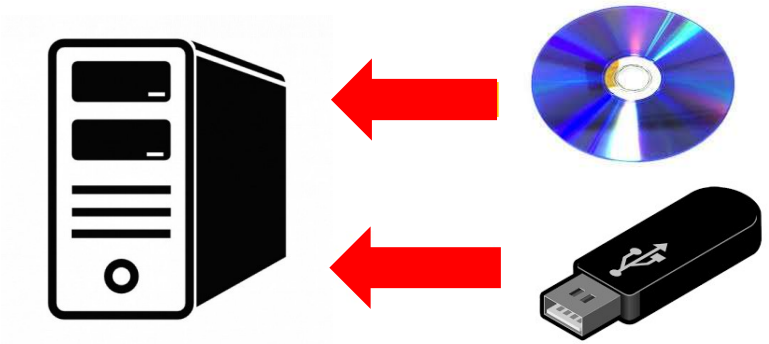
Minimum hardware requirements for Windows Server 2022:

Component	Requirement
Processor architecture	64 bit
Processor speed	1.4 gigahertz (GHz)
RAM	512 MB (2 GB for Desktop Experience)
Hard drive space	32 GB
Network	1 gigabit per second throughput

Overview of deployment options (1 of 2)

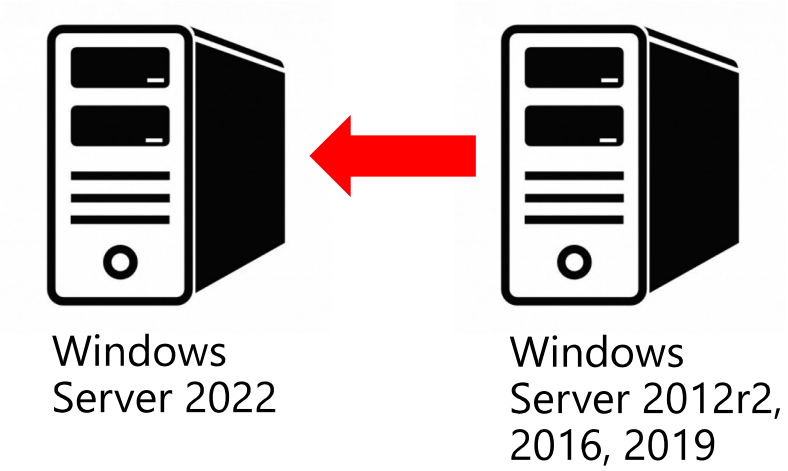
Clean install:

- Boot the physical machine or virtual machine from the Windows Server 2022 media
- Choose the installation language, time and currency formats, and keyboard layout
- Choose the architecture (either Standard or Datacenter) with or without Desktop Experience
- Accept the license
- Choose custom installation
- Choose the volume that will host the installation



Overview of deployment options (2 of 2)

- In-place upgrade
  - Insert the disk or mount the ISO of Windows Server 2022 media and then run **Setup.exe**
  - Choose the architecture (either **Standard** or **Datacenter**) with or without **Desktop Experience**
  - Accept the license
  - Choose what to keep: personal files and apps, or nothing



Demo: Windows Server 2022 Installation

Prerequisite: Create a new virtual machine

- ❑ Name = RTS-DC1
- ❑ Generation =Generation 2
- ❑ Memory = 2048 MB (2GB) recommended 4096 MB (4GB)
- ❑ Virtual Switch = Name: External. Type: External
- ❑ VHD: Accept default
- ❑ ISO: Browse to downloaded Windows Server 2022 ISO file

VirtualBox Demo: https://RTSnetworking.com/demo

Servicing channels for Windows Server

You can use servicing channels to choose whether new features and functionality will be delivered regularly during a server's production lifespan, or when to move to a new server version

- There are two release channels:
  - Long-Term Servicing Channel
    - A new major version of Windows Server is released every 2-3 years. Users are entitled to 5 years of mainstream support and 5 years of extended support. This channel is appropriate for systems that require a longer servicing option and functional stability. The Long-Term Servicing Channel will continue to receive security and non-security updates, but it will not receive the new features and functionality.
  - Semi-Annual Channel
    - The Semi-Annual Channel is perfect for customers who are innovating quickly to take advantage of new operating system capabilities at a faster pace, focused in on containers and microservices. Windows Server products in the Semi-Annual Channel will have new releases available twice a year, in spring and fall. Each release in this channel will be supported for 18 months from the initial release.

Licensing and activation models for Windows Server

Licensing for Windows Server **Standard** and **Datacenter** is based on the number of cores, not processors

- Each Windows Server has the following minimum license requirement:
  - All physical cores must be licensed
  - There must be 8 core licenses per processor
  - There must be 16 core licenses per server

- Client Access Licenses (CALs) are required for each user or device that connects to the server for any purpose

MICROSOFT

Microsoft Windows Server 2022 Standard - 16 Core License

SKU: P73-08328

Trusted Return Policy

$577.99

☆☆☆☆☆ No reviews

DETAILS (View full description)

- Virtualize by enabling the optional Hyper-V hypervisor role (included)
- Includes Two (2) Virtual Machines (Minimum of 16-Cores Required)
- Server Standard 2022 requires CALs, which are not included unless stated
- *Microsoft requires a minimum of 16-cores per server and at least 8-cores per processor.
- Comprehensive Price Quote delivered within 30 minutes or less, volume discounts available

TOTAL: **$577.99**

QUANTITY: − 1 +

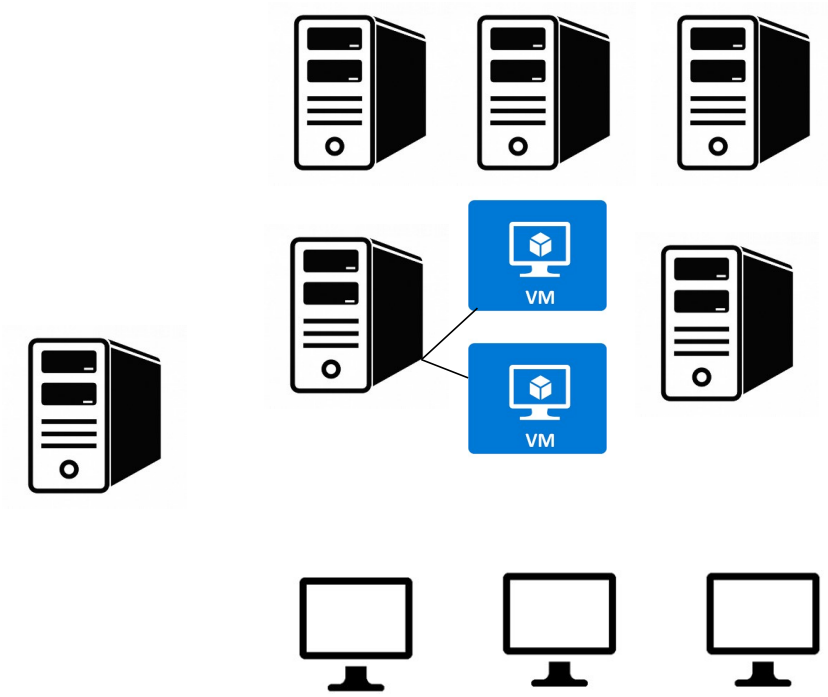
ADD TO CART

BUY IT NOW

Licensing and activation models for Windows Server

To ensure that your organization has the proper licenses, you must activate every copy of Windows Server that you install

- Windows Server activation methods:
  - Manual activation requires a product key
  - Automatic activation options:
    - Key Management Services
    - Active Directory-based activation
    - Multiple Activation Key
    - Automatic virtual machine activation



Lesson 2 overview

In this lesson, you'll learn about the differences between Server Core and Windows Server with Desktop Experience, and when one is the preferred option

- Topics
  - Server Core vs. Windows Server with Desktop Experience
  - Server Core installation and post-installation tasks
  - Install features on demand
  - Use sconfig in Server Core

Server Core vs Desktop Experience

Server Core is a minimal installation option for Windows Server that does not include the traditional graphical user interface (GUI). Instead, it provides a command-line interface and support for remote management tools. This makes it a more lightweight and secure option for running server workloads, as it reduces the attack surface and minimizes the resources required for running the operating system.

Desktop Experience is the full installation option for Windows that includes the GUI and all the features and tools typically found in a desktop operating system. This installation option is designed for users who need a more familiar interface and access to applications using a GUI

Server Core vs Desktop Experience

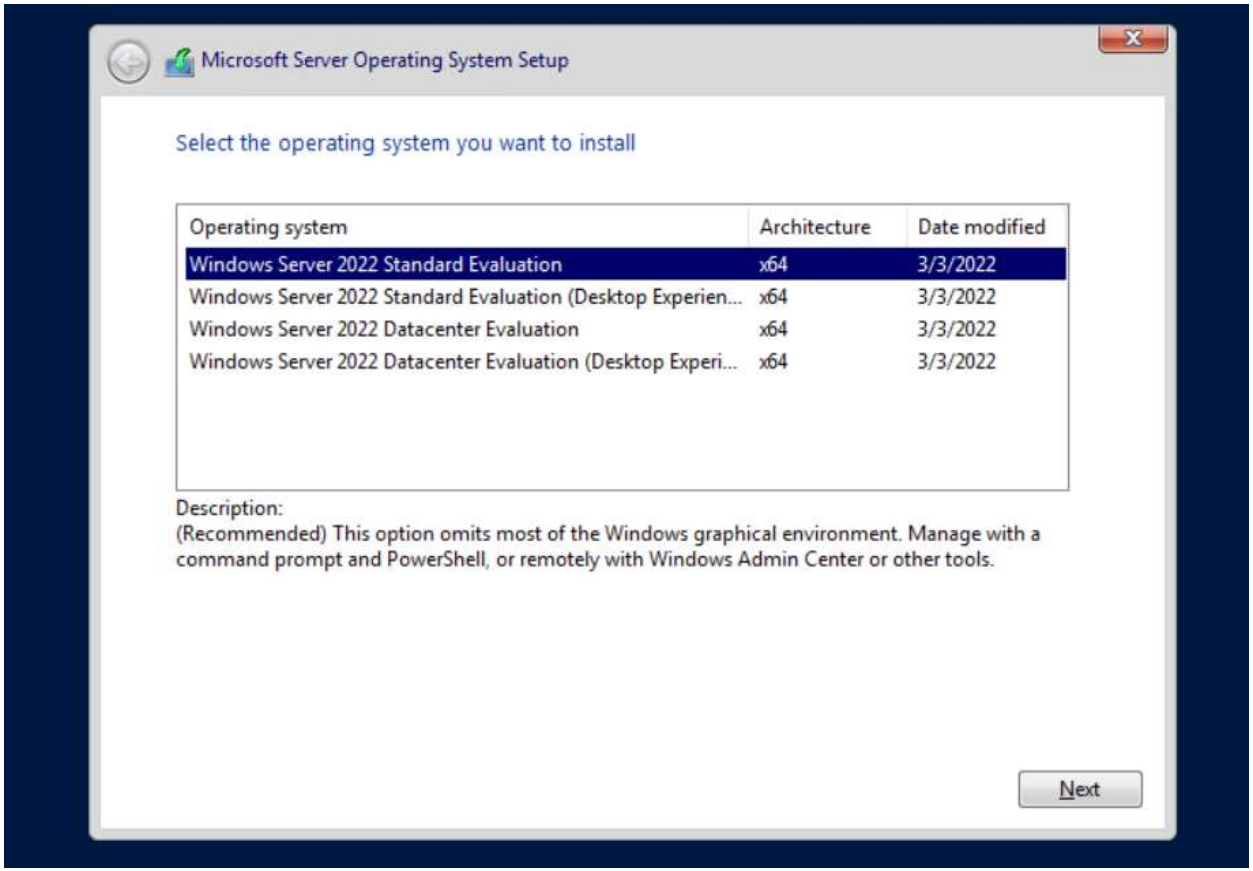
The following table lists the major advantages and disadvantages of Server Core

Advantages	Disadvantages
Small footprint that uses fewer server resources and less disk space, as little as 4 GB for a basic installation	Some applications are not supported on a Server Core installation.
Because Server Core installs fewer components, there are fewer software updates. This reduces the number of monthly restarts required and the time required for you to service Server Core.	Some roles and role services are not available.
The small attack surface makes Server Core much less vulnerable to exploits.	No local Graphical User Interface (GUI)

Server Core installation and post-installation tasks

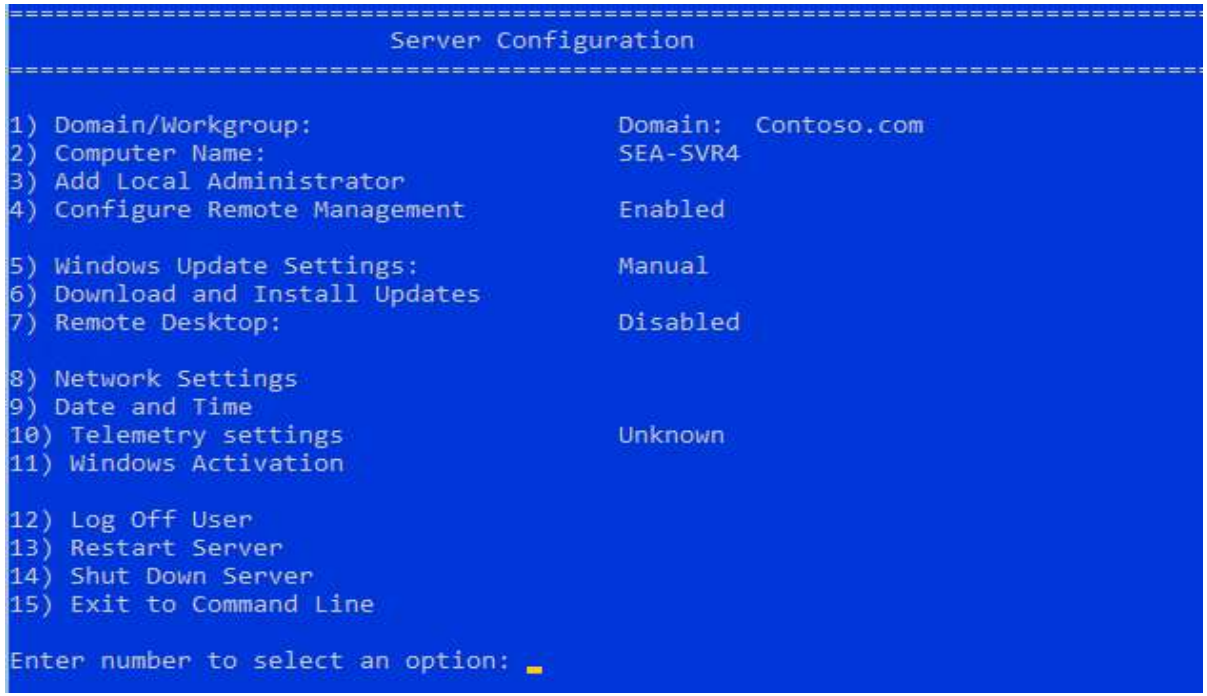
To install Server Core:

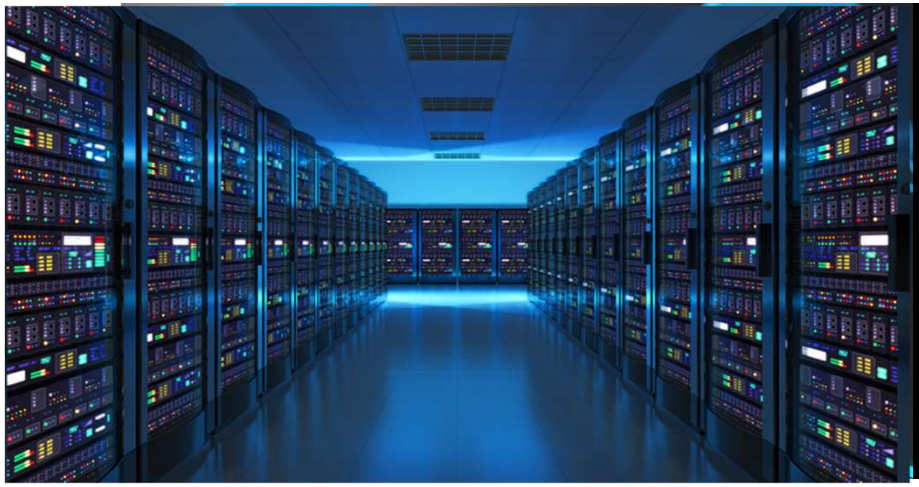
- Connect to the installation source
- Choose:
  - Language
  - Time and currency
  - Keyboard
- Select the operating system to install
- Accept license
- Choose installation type
  - Upgrade
  - Custom
- Choose install disk
- Provide admin password



Using sconfig in Server Core

- sconfig is a menu-based utility that allows you configure Server Core
- sconfig eliminates the need for scripting initial configuration settings





Module 2:

Active Directory Domain Services on Windows Server 2022

Module overview

This module introduces you to Active Directory on Windows Server 2022

Lessons

- Overview of AD DS (Active Directory Domain Services)
- Deploying domain controllers on Windows Server 2022
- Implementing Group Policy

Lesson 1

In this lesson, you'll learn about Workgroups, Domains, and Active Directory components.

Topics:

- Understanding workgroups and domains
- Active Directory terms
- Active Directory Domains and Forests
- Understanding Active Directory objects
- Understanding Domain Controllers
- Global Catalog

Types of Networks

WORKGROUP

No Centralized Authentication

No Centralized Administration

Max of 20 computers supported

Low Security

DOMAIN

Centralized Authentication

Centralized Administration

Unlimited number of computers

High Security

Domain vs Workgroup (Non-Technical way to think)

Domain

Parents

House Rules set by parents

Children

Workgroup

Each person sets their own rules

Children

Active Directory Domain Services (AD DS)Terms

AD DS is composed of both logical and physical components

Logical components	Physical components
• Domains • Domain trees • Forests • OUs • Containers	• Domain Controllers • Read-only Domain Controllers

AD DS Domains and Forests

- A domain:
  - A repository for User, Computers and other objects
  - A replication boundary
  - An administrative boundary

- A domain controller is a server that has Active Directory Domain Services (AD DS) installed

AD DS Domains and Forests

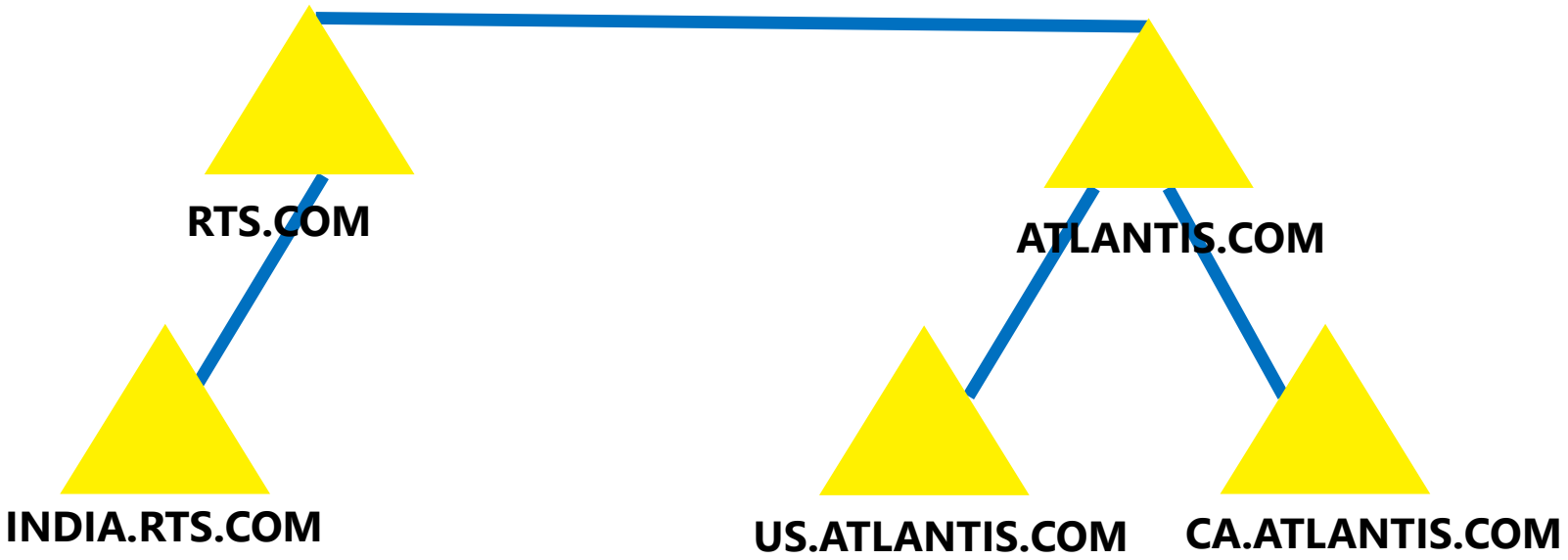
RTS.COM

AD DS Domains and Forests

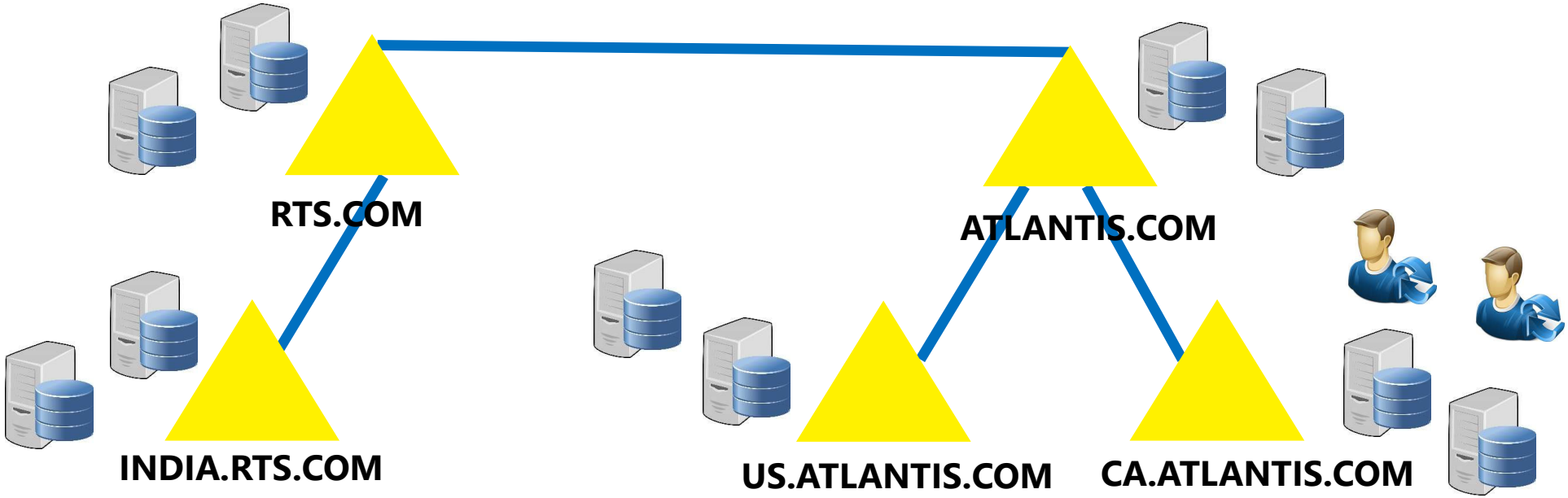
- A forest:
  - Is a security boundary
  - One or more domains that share a trust relationship

- Trust relationships:
  - A relationship between domains that allows access to resources in other domains within the same forest

AD DS Domains and Forests



AD DS Forest


RTS.COM
ATLANTIS.COM
INDIA.RTS.COM
US.ATLANTIS.COM
CA.ATLANTIS.COM

RTS-Core (Server 2022)

IP Address: 192.168.1.252
Subnet Mask: 255.255.255.0
Default Gateway: (Blank)
Preferred DNS: 192.168.1.250
Alternate DNS: (Blank)

RTS-DC1
Domain Controller/ DNS Server (Server 2022)

IP Address: 192.168.1.250
Subnet Mask: 255.255.255.0
Default Gateway: (Blank)
Preferred DNS: 192.168.1.250
Alternate DNS: (Blank)

RTS-SVR1 (Server 2022)

IP Address: 192.168.1.251
Subnet Mask: 255.255.255.0
Default Gateway: (Blank)
Preferred DNS: 192.168.1.250
Alternate DNS: (Blank)

AD DS objects

- User objects
  - Authentication of the user at logon
  - Access control
- Group objects
  - Simplify assigning permissions
- Computer objects
  - Authentication of the computer at startup

Organizational Units and Containers

- Use containers to group objects within a domain:
  - You cannot apply GPOs to containers
  - Containers are used for system objects and as the default location for new objects

Container

- Create OUs to:
  - Configure objects by assigning GPOs to them
  - Delegate administrative permissions

Organizational Unit

Domain Controllers

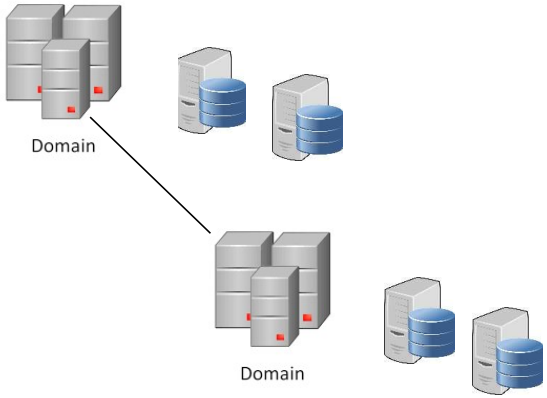
Domain controllers:

- Are servers that host the AD DS database (**Ntds.dit**) and **SYSVOL**
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain

Domain

What is the Global Catalog?

- The global catalog:
  - Hosts a partial attribute set for other domains in the forest
  - Supports queries for objects throughout the forest
- In a single domain, you should configure all the domain controllers to hold a copy of the global catalog
- When you have multiple sites, you should also make at least one domain controller at each site a global catalog server



Lesson 2

In this lesson, you'll learn about configuring Group Policy for client, user, and server administration.

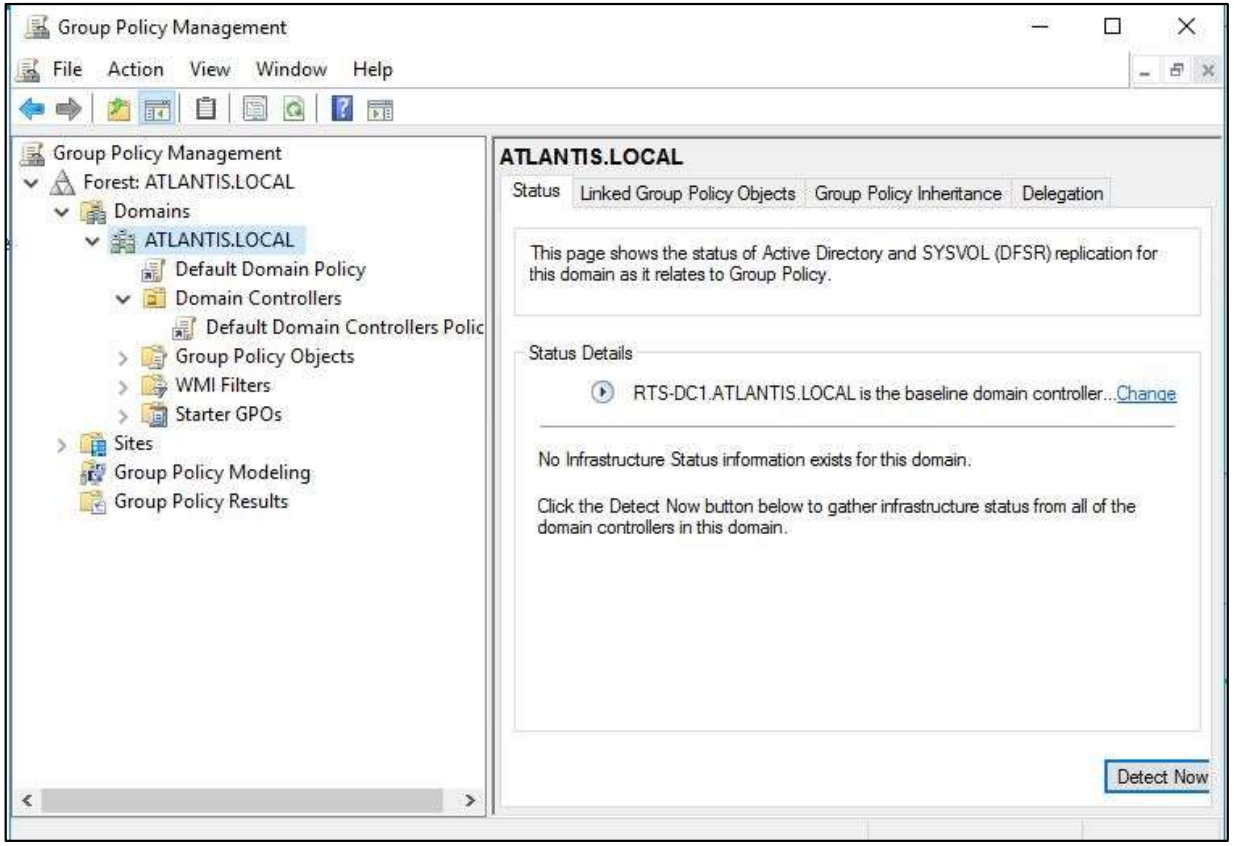
Topics:

- ❑ What are Group Policy Objects?
- ❑ Understanding Domain-based Group Policy Objects
- ❑ Implementing Group Policy Preferences
- ❑ Implementing Group Policy Inheritance
- ❑ Group Policy Processing
- ❑ Using GPupdate
- ❑ Using GPresult

What are GPOs?

- Group Policy is a powerful administrative tool
- You can use it to enforce various types of settings to a large number of users and computers
- Typically, you use GPOs to:
  - Apply security settings
  - Manage desktop application settings
  - Deploy application software
  - Manage Folder Redirection
  - Configure network settings

What are Domain-based GPOs?



What are Group Policy Preferences?

Group Policy Preferences are a collection of Group Policy client-side extensions that deliver preference settings to domain-joined computers.

Preference settings differ from policy settings because users have a choice to alter the administrative configuration. Policy settings administratively enforce setting, which restricts user choice.

Preferences can be targeted to specific groups, operating systems, IP addresses, MAC addresses, and more.

Group Policy Preferences

F5= Enable all settings

F6= Enable selected setting

F7= Disable selected setting

F8= Disable all settings

Overview of GPO scope and inheritance

GPOs are processed on a client computer in the following order:

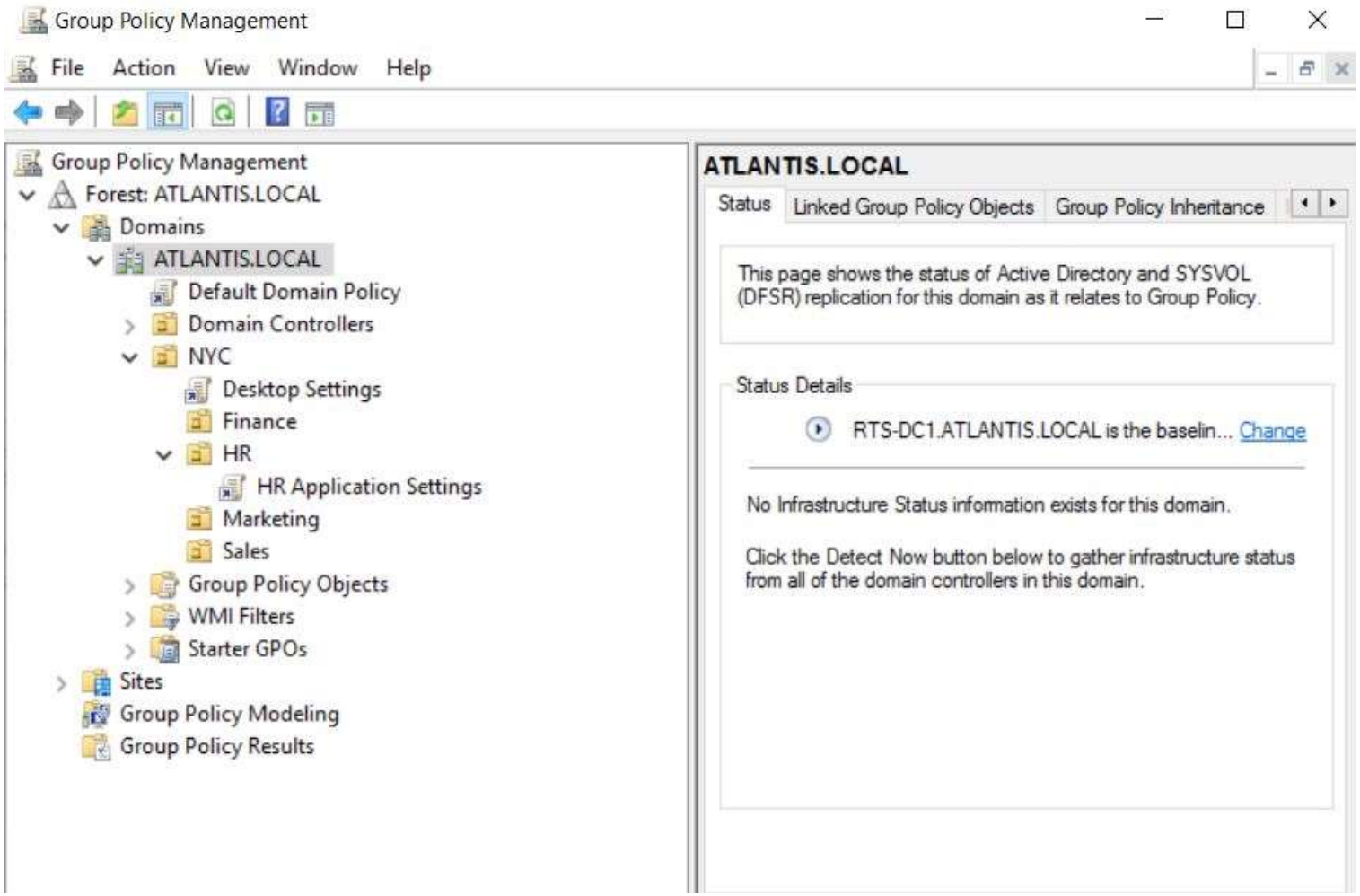
1. Local GPOs
2. Site-level GPOs
3. Domain-level GPOs
4. Organizational Unit GPOs

Altering Group Policy Processing

Block inheritance

Enforced

Security filtering



What is an Active Directory Site?

GPUpdate

What is GPUpdate?

Gpupdate is a command-line utility from Microsoft that comes with all versions of the Windows operating system. It's a utility that controls the application of ***group policy objects (GPOs)*** on assigned Active Directory computers.

Gpupdate /Force will process all GPOs regardless if they have changed or not

GPResult

Verify the GPOs that are currently applying to a user and computer account

Examine the settings that apply to the user and computer and determine which GPO applied the setting

Lesson 3 overview

In this lesson, you'll learn about Windows Server administration best practices and the tools used for management.

- Topics
  - Overview of the least-privilege administration concept
  - Implementing Delegated privileges
  - Deploying Jump servers
  - Overview of the Windows Server Admin Center
  - Exploring Server Manager
  - Implementing Remote Server Administration Tools (RSAT)
  - Introduction to Windows PowerShell

Overview of the least-privilege administration concept

Most security breaches or data loss incidents are the result of human error, malicious activity, or a combination of both. Least privilege is the concept of restricting access rights for users and computing processes to only those resources absolutely required to perform their job roles.

The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers.

Day to day standard user account for IT admins

Bob Ross
(non-admin account)

Bob Ross
(admin account)

New Users

Full admin account only used to perform administration functions

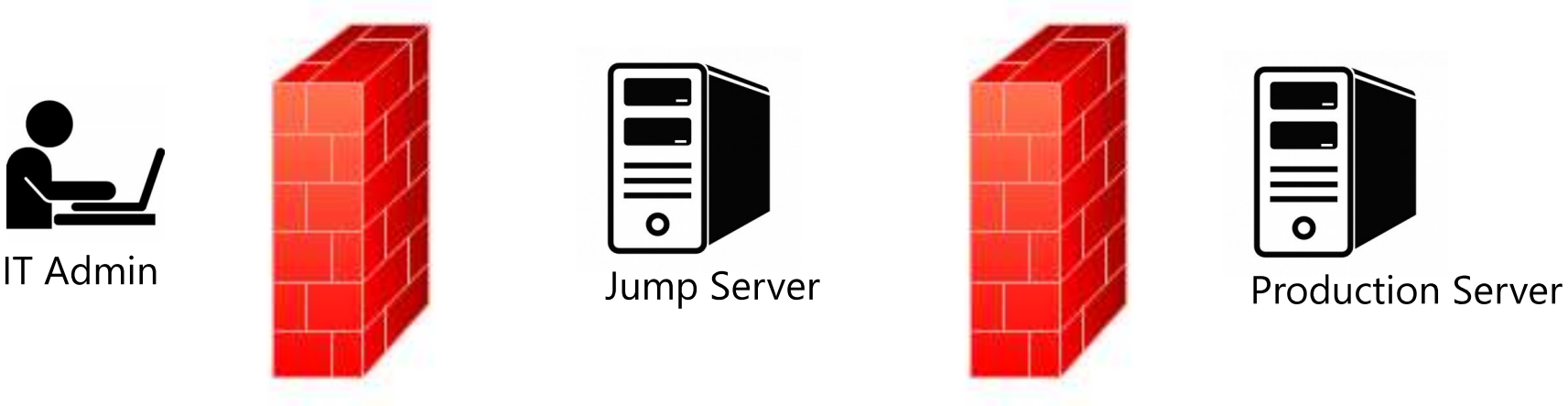
Domain Controller

Delegated privileges

- Accounts that are members of high-privilege groups such as **Enterprise Admins** and **Domain Admins** need to be guarded, but occasionally non-admins need rights to perform certain functions, such as resetting passwords or modifying group memberships.
- Built-in groups with pre-defined admin rights exist to allow users to perform specific admin tasks. If those groups do not suit your needs, you can delegate more granular permissions by using the **Delegation of Control Wizard**.
  - The wizard has pre-defined tasks that can be assigned to users or groups, or custom permissions can be assigned.

Jump servers

- A jump server is a hardened server used to access and manage devices in a different security zone, such as between an internal network and a perimeter network



Overview of Windows Admin Center

- Windows Admin Center consolidates multiple admin tools into a single console that can be easily deployed and accessed through a web interface
- Windows Admin Center is a modular web application comprised of the following four modules:
  - Server manager
  - Failover clusters
  - Hyper-converged clusters
  - Windows 10 and Windows 11 clients

Server Manager

- **Server Manager** allows server administrators to:
  - Manage the local server and remotely manage multiple servers
  - Configure the local server
  - Query event logs
  - Monitor status of services
  - Perform best practice analysis
  - Check performance monitors
- **Server Manager** initially opens to the dashboard, which provides quick access to:
  - Add roles and features
  - Add other servers to manage
  - Create a server group
  - Connect this server to cloud services

Remote Server Administration Tools

- To enable IT administrators to remotely manage roles and features in Windows Server from a computer that is running Windows 11 or Windows 10, use **RSAT**
- **RSAT** include:
  - Active Directory Domain Services tools
  - DHCP server tools
  - DNS server tools
  - File services tools
  - Group Policy management tools

Windows PowerShell

- Windows PowerShell is a command line shell and scripting language
- Windows PowerShell cmdlets execute in a Windows PowerShell console or can be executed as PowerShell scripts
- Cmdlets:
  - Are small commands that perform specific functions
- Modules:
  - Cmdlets specific to a product are packaged together and installed as modules
  - Some are installed with the product and some need to be added manually

Windows PowerShell

- PowerShell Console
  - Run PowerShell commands and execute scripts
- PowerShell ISE
  - PowerShell Integrated Scripting Environment (ISE) is a graphical user interface–based tool that allows you to:
  - Run commands, create, modify and execute scripts
- Windows PowerShell remote management:
  - Allows Windows PowerShell to remotely run cmdlets on other Windows systems

Windows PowerShell vs CMD Prompt

CMD Prompt

Ping

Ping rtsnetworking.com

Ping –t rtsnetworking.com

IPconfig

Ipconfig /all

DiskPart utility

Unique syntax only used in DiskPart

PowerShell

Verb-Noun

Test-connection rtsnetworking.com

Test-connection rtsnetworking.com –count 10

Get-eventlog

Get-eventlog –LogName System

PowerShell Help

Get-help

Get-help *event*

Get-help *eventlog*

Get-help get-eventlog

Get-help get-eventlog -detailed

Get-help get-eventlog -examples

Get-help get-eventlog -full

Get-help get-eventlog –online

Update-help

Save-help

Module 3:

Managing Dynamic Host Configuration Protocol (DHCP)

Lesson 1 overview

Topics:

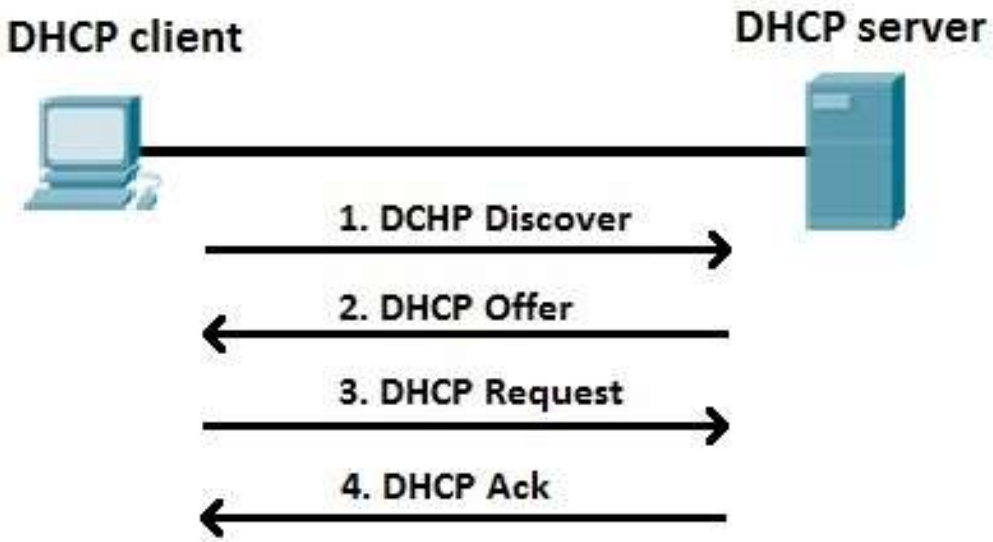
- Overview of the DHCP role
- Install and configure the DHCP role
- Configure DHCP scopes
- DHCP AD DS authorization
- DHCP Failover for high availability

Overview of the DHCP role

DHCP automates management of IP configuration on clients and devices

DHCP lease renewal is attempted at:

- Startup
- 50% of lease time
- 87.5% of lease time



Install and configure the DHCP role

To install the DHCP role:

- **Windows Admin Center > Roles and Features**
- **Server Manager**
- **Add-WindowsFeature DHCP -IncludeManagementTools**

To manage a DHCP server by using Windows Admin Center, you must install the DHCP PowerShell tools

Install and configure the DHCP role

DHCP local security groups:

- DHCP Administrators
- DHCP Users

To create the DHCP local security groups:

- **Server Manager > Post-Install Configuration Wizard**
- **Add-DhcpServerSecurityGroup -Computer DhcpServerName**

Configure DHCP scopes

Properties of a DHCP scope:

- Name (mandatory)
- IP address range (mandatory)
- Subnet mask (mandatory)
- Exclusions
- Delay
- Lease duration
- Options
- Activation

Option code	Name
3	Router (Default Gateway)
6	DNS servers
15	DNS domain name

DHCP AD DS authorization

A DHCP server on Windows Server must be authorized in AD DS to lease IP addresses:

- To authorize a DHCP server by using Windows PowerShell, run:

  `Add-DHCPServerinDC <name or IP address of DHCP server>`

A standalone server with DHCP will not lease IP addresses if an authorized DHCP server is detected

Non-Windows DHCP servers and devices will function regardless of authorization

DHCP High availability

Split scopes:

- Involve two DHCP servers that are configured with non-overlapping scopes

DHCP failover:

- Scopes are replicated from one DHCP to another DHCP partner
- Strongly preferred to implement high availability for DHCP

Failover configuration modes:

- Load balance
- Hot standby

Module 4:

Managing Domain Name System (DNS)

Lesson 1 overview

Topics:

- DNS components
- DNS records
- DNS zones
- Create records in DNS
- Configure DNS zones
- DNS forwarding
- Integrating DNS with Active Directory

DNS components

DNS domain names:

- Are a portion of DNS namespace
- Can be public or private

DNS servers:

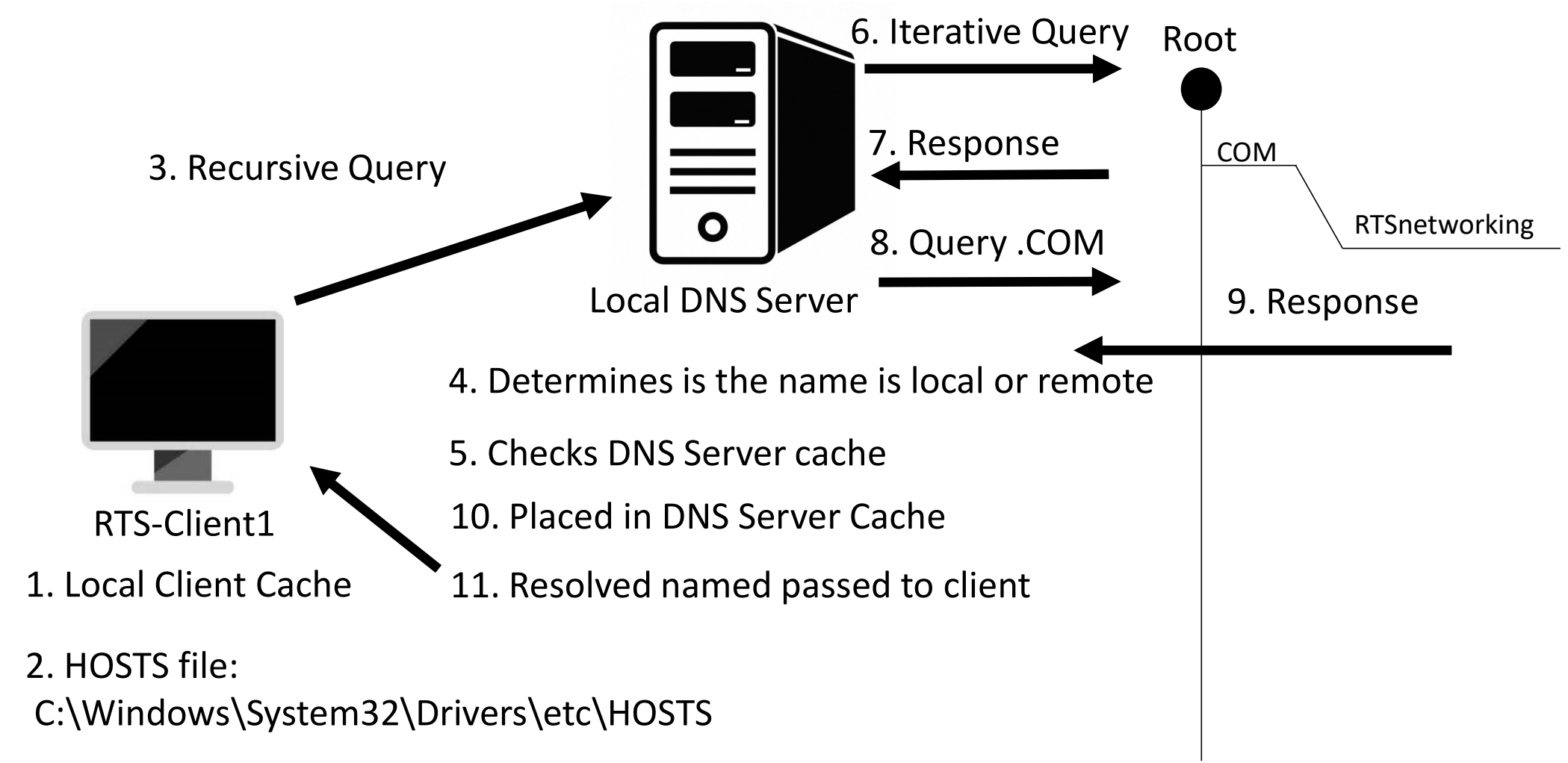
- Respond to name resolution requests
- Stores resource records locally in a database on the DNS server

DNS zones and resource records:

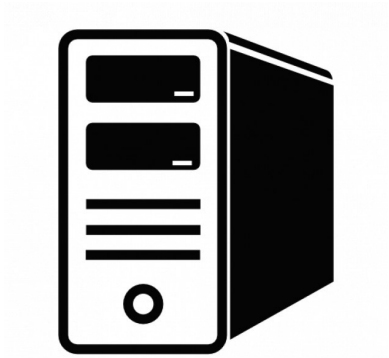
- A zone is a local copy of a DNS namespace on a DNS server
- Resource records are created and stored in a zone

DNS resolvers:

- Request DNS information from DNS servers
- Cache results

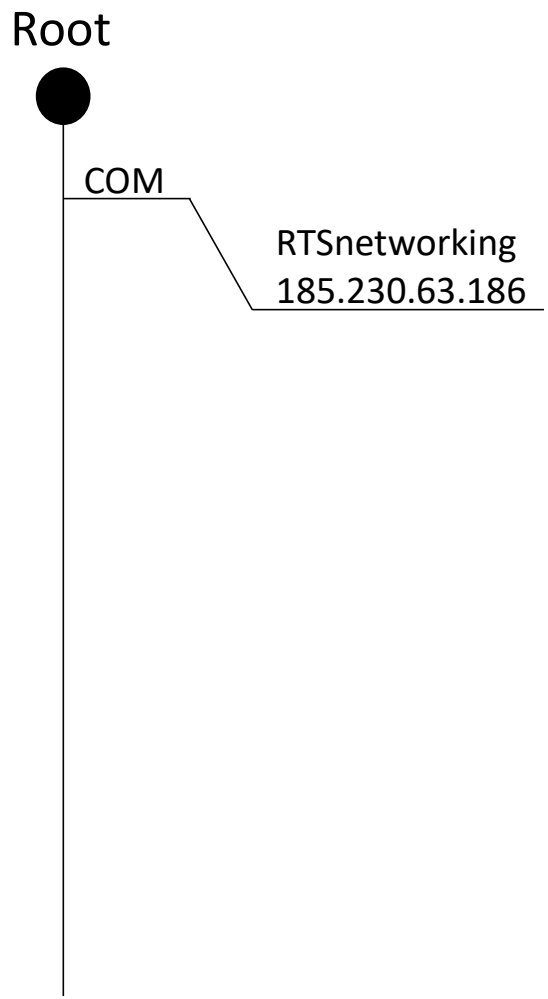

6. Iterative Query
Root
7. Response
3. Recursive Query
COM
RTSnetworking
8. Query .COM
Local DNS Server
9. Response
4. Determines is the name is local or remote
5. Checks DNS Server cache
RTS-Client1
10. Placed in DNS Server Cache
1. Local Client Cache
11. Resolved named passed to client
2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

www.RTSnetworking.com

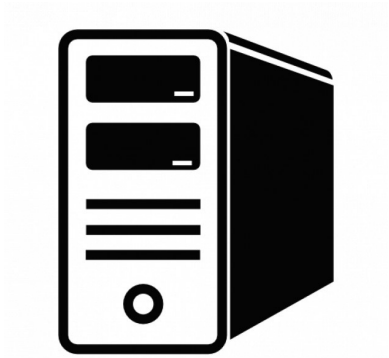


Local DNS Server

RTS-Client1



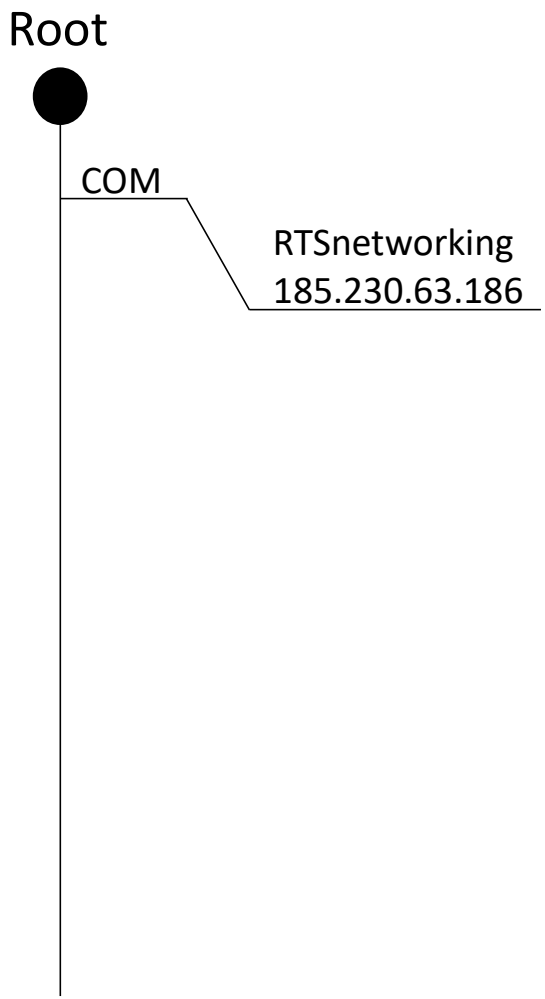
www.RTSnetworking.com



Local DNS Server

RTS-Client1

1. Local Client Cache



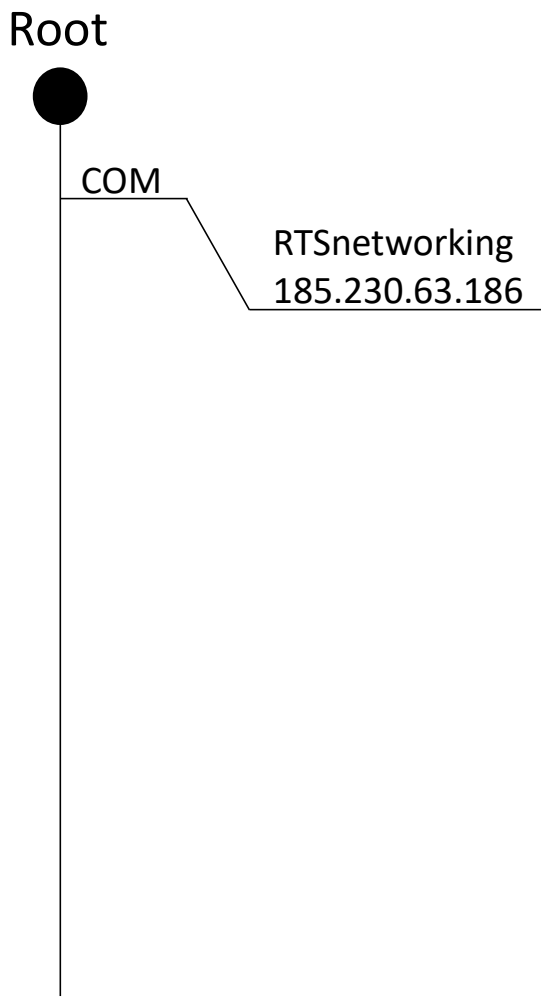
www.RTSnetworking.com

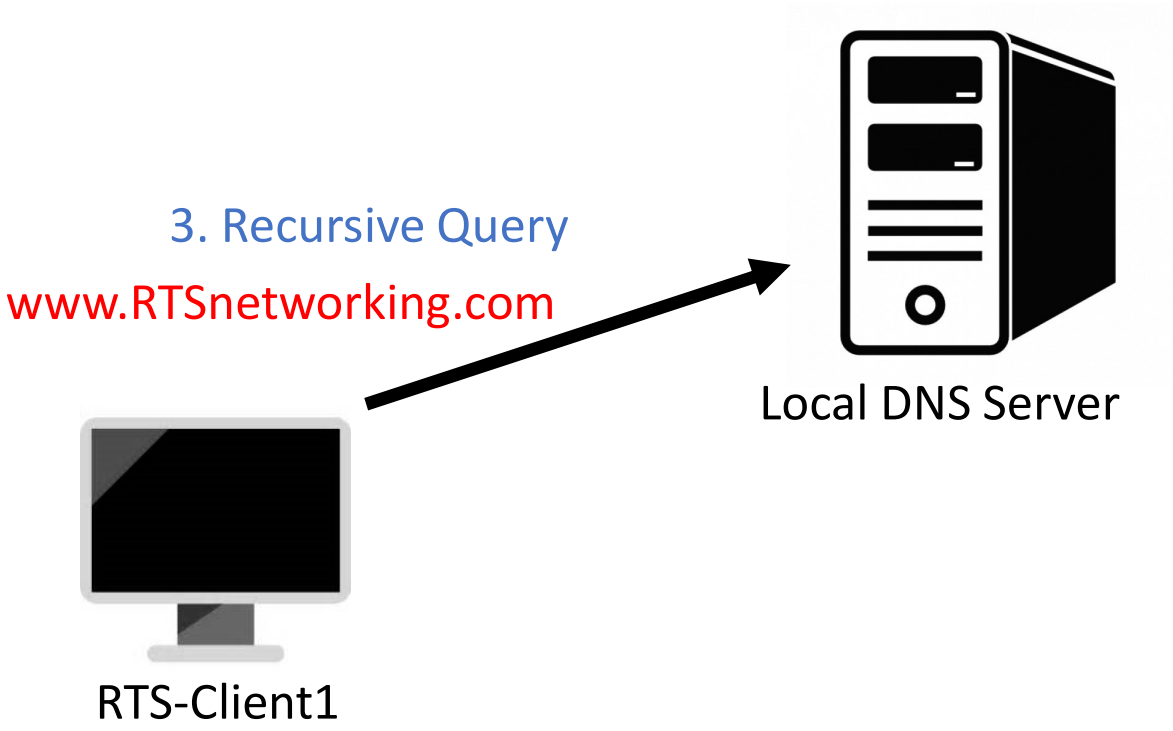
Local DNS Server

RTS-Client1

1. Local Client Cache

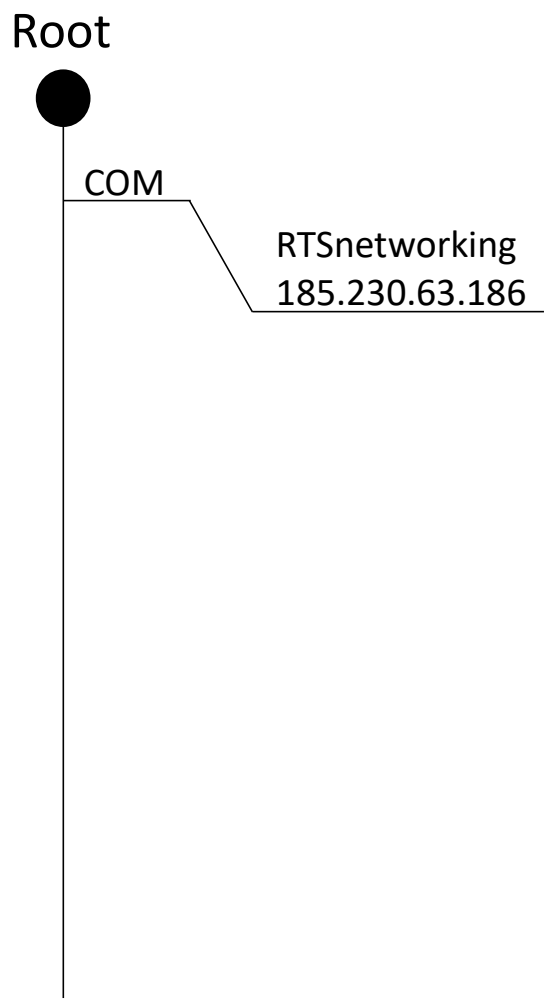
2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

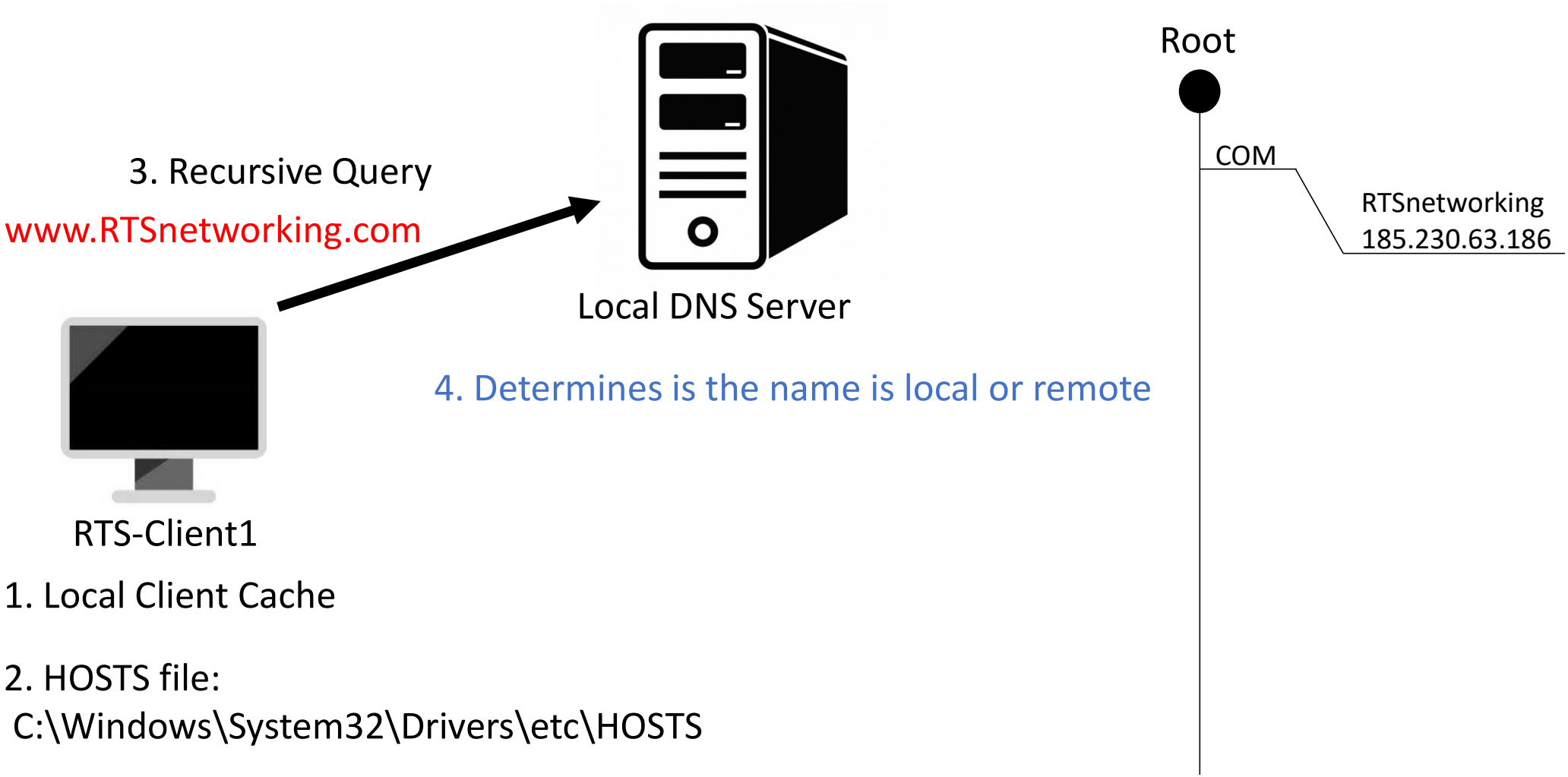




1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

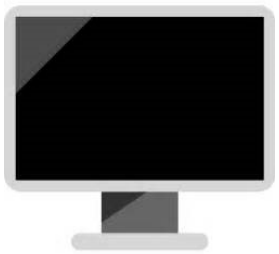



Root
COM
RTSnetworking
185.230.63.186
3. Recursive Query
www.RTSnetworking.com
Local DNS Server
4. Determines is the name is local or remote
RTS-Client1
1. Local Client Cache
2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

Local DNS Server

3. Recursive Query

www.RTSnetworking.com



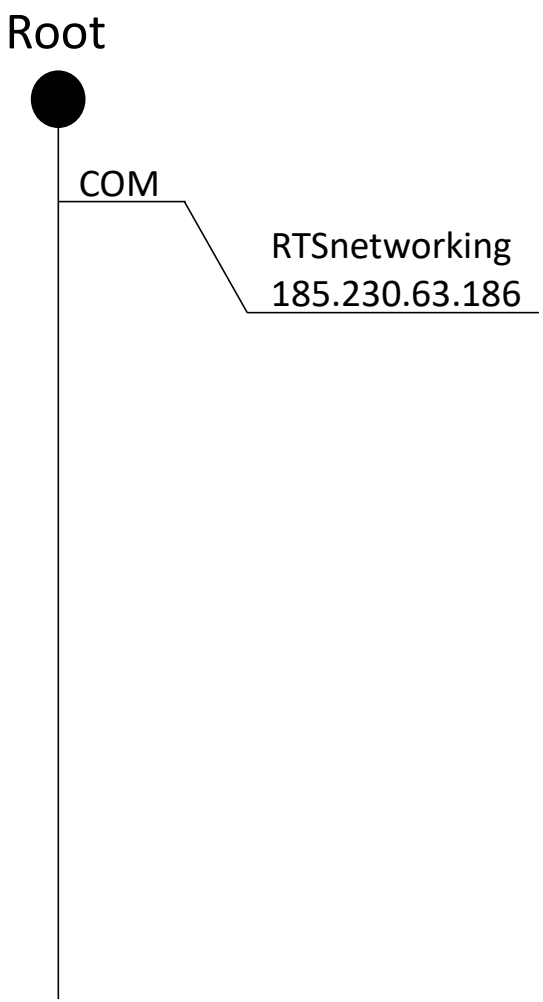
RTS-Client1

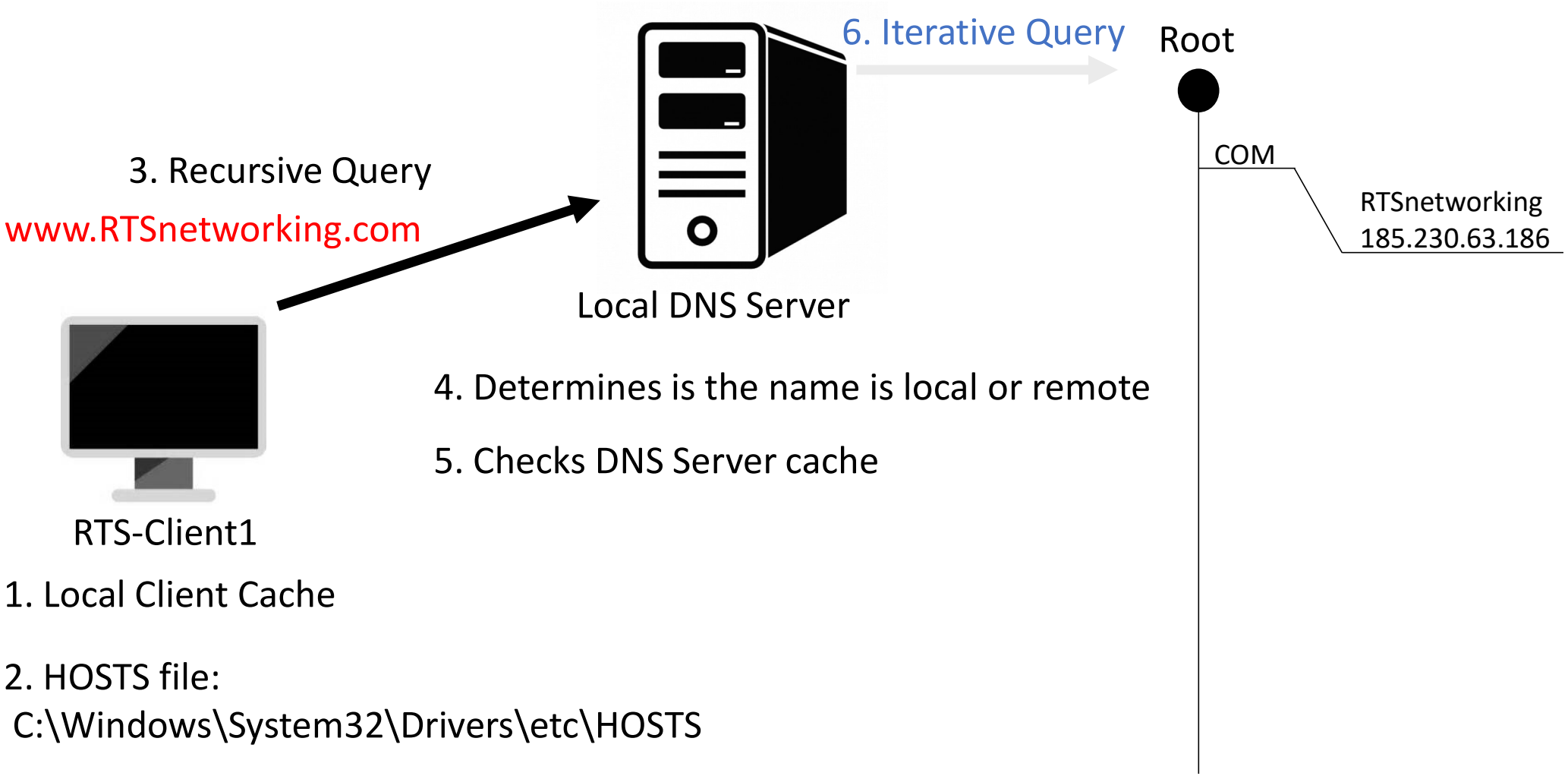
4. Determines is the name is local or remote

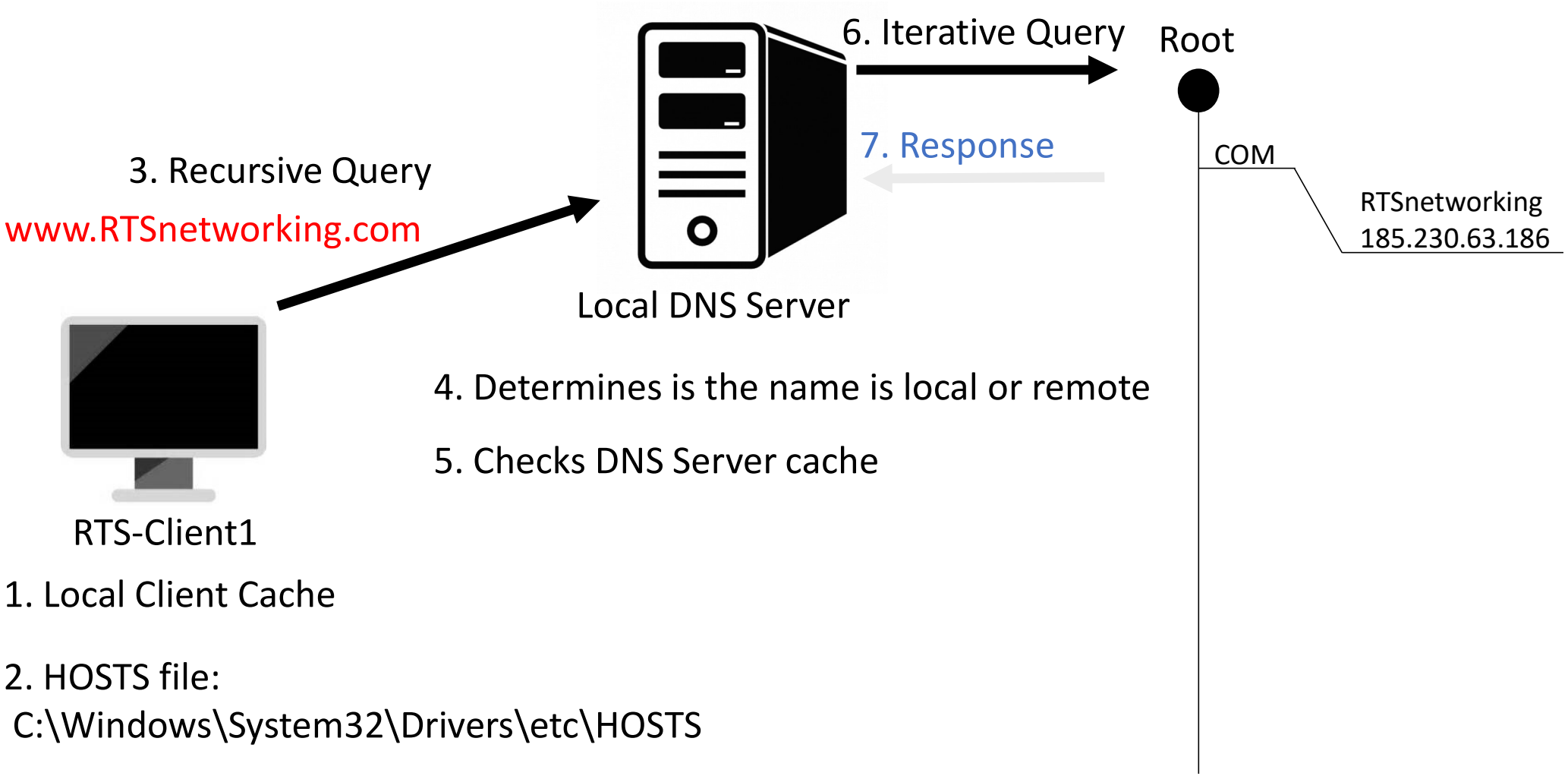
5. Checks DNS Server cache

1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

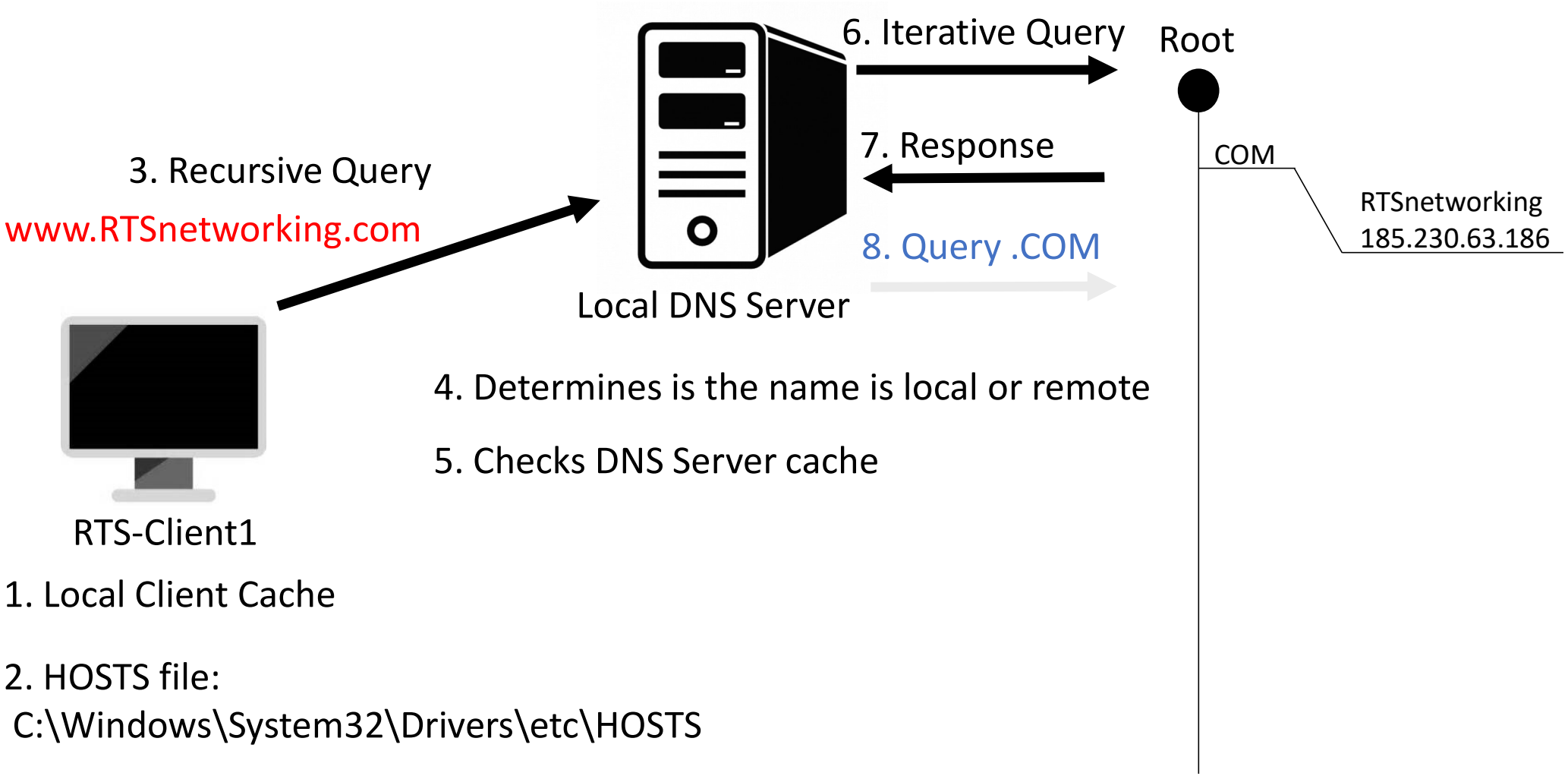



6. Iterative Query
Root
COM
RTSnetworking
185.230.63.186
3. Recursive Query
www.RTSnetworking.com
Local DNS Server
4. Determines is the name is local or remote
5. Checks DNS Server cache
RTS-Client1
1. Local Client Cache
2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS



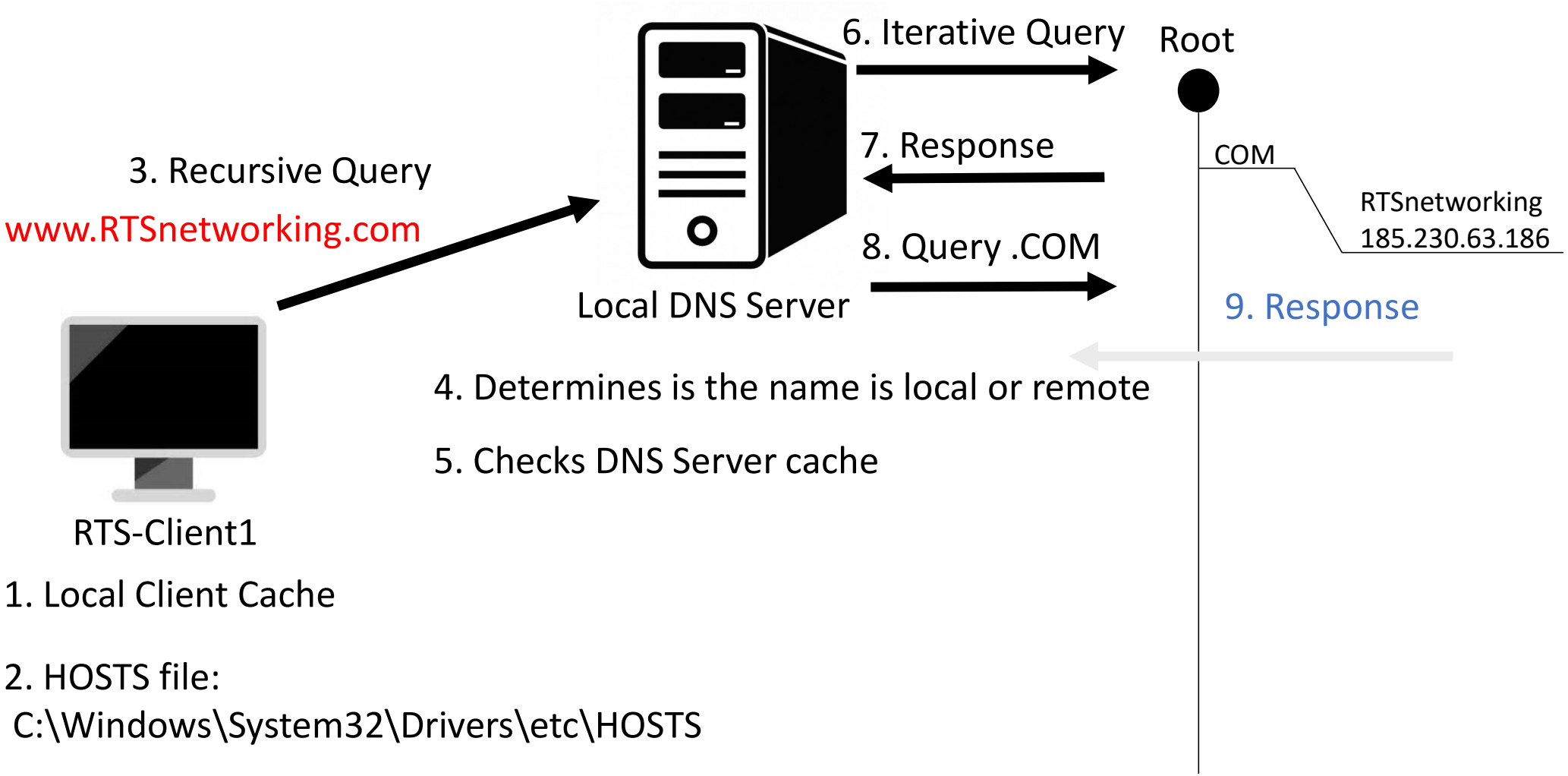
1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS



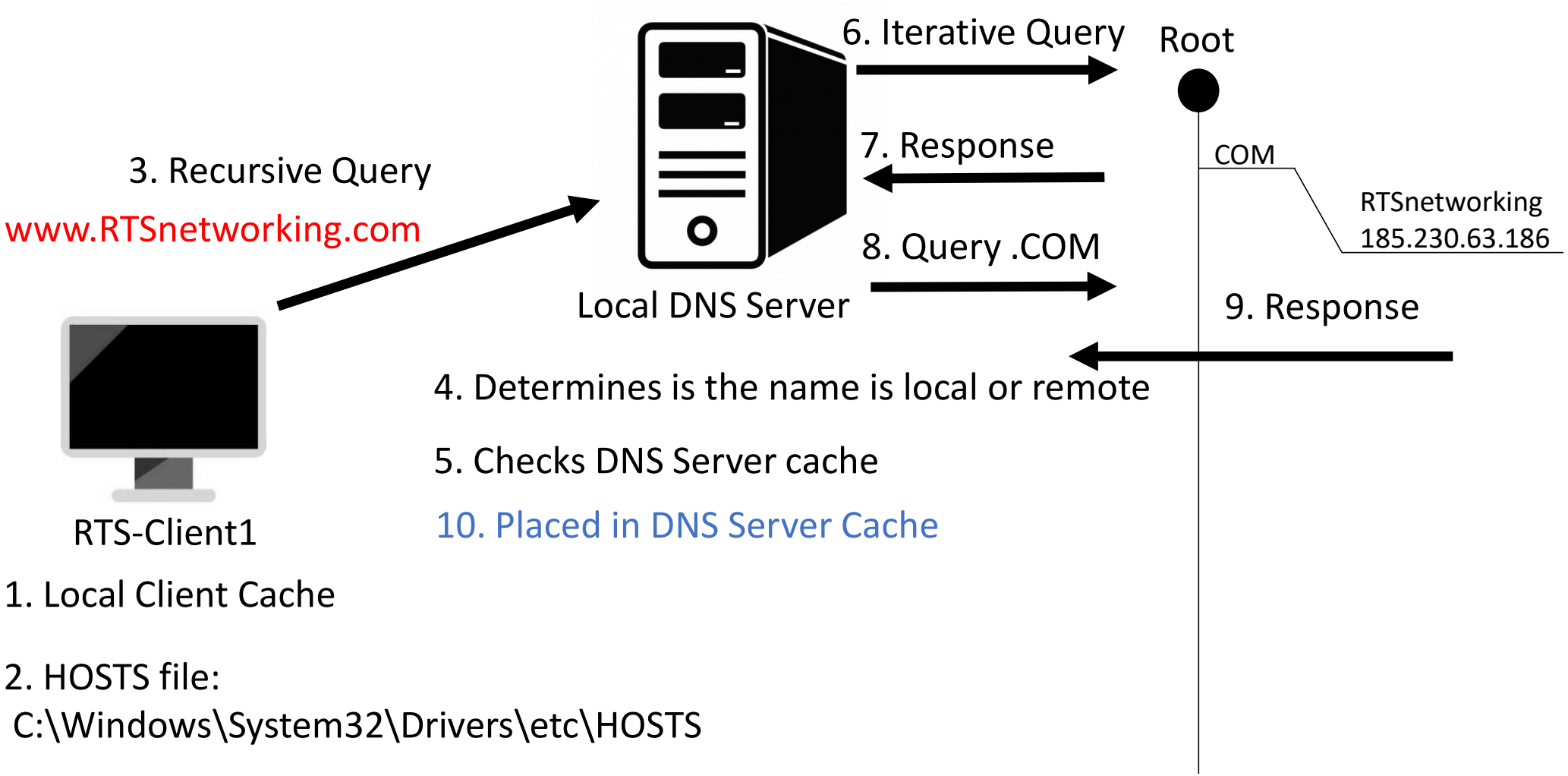
1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS



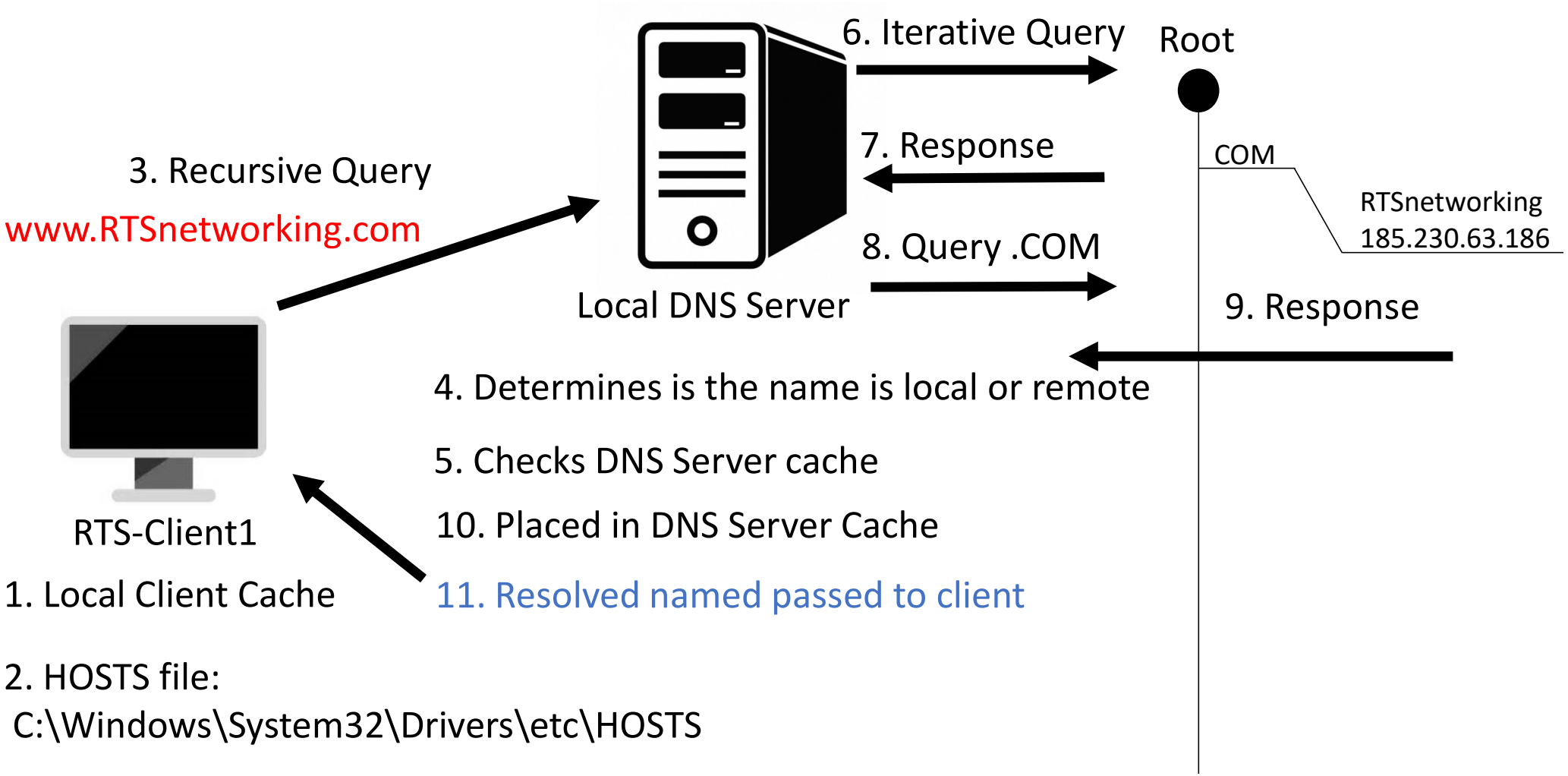
1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS



1. Local Client Cache

2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS


6. Iterative Query
Root
7. Response
COM
RTSnetworking
185.230.63.186
3. Recursive Query
www.RTSnetworking.com
8. Query .COM
Local DNS Server
9. Response
4. Determines is the name is local or remote
5. Checks DNS Server cache
RTS-Client1
10. Placed in DNS Server Cache
1. Local Client Cache
11. Resolved named passed to client
2. HOSTS file:
C:\Windows\System32\Drivers\etc\HOSTS

DNS records

Forward lookup zones include:

- Host (A)
- Host (AAAA)
- Alias (CNAME)
- Service location (SRV)
- Pointer (PTR)

Create records in DNS

Manual creation methods:

- Windows Admin Center
- DNS manager
- Windows PowerShell

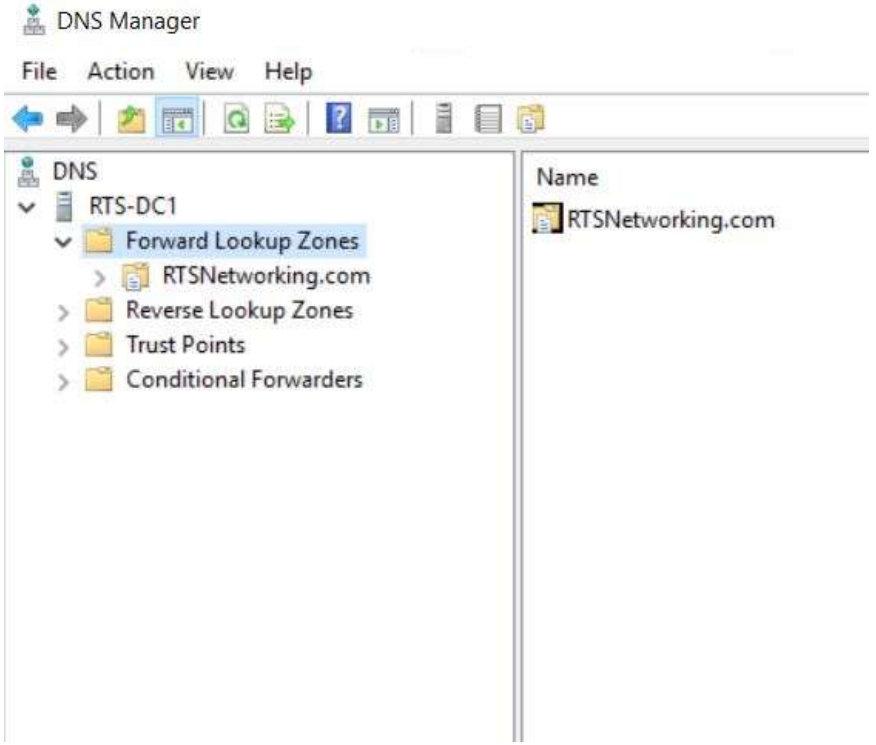
Dynamic creation:

- Clients register name and IP address in a zone

DNS zones

A DNS zone is the portion of a DNS namespace hosted on a DNS server:

- Forward lookup zones:
  - Resolve names to IP addresses
  - Can contain many other record types
- Reverse lookup zones:
  - Resolve IP addresses to names
  - Are in the **in-addr.arpa** namespace



DNS zones

Primary zones:

- Are authoritative for a portion of a DNS namespace
- Are where resource records are created

Secondary zones

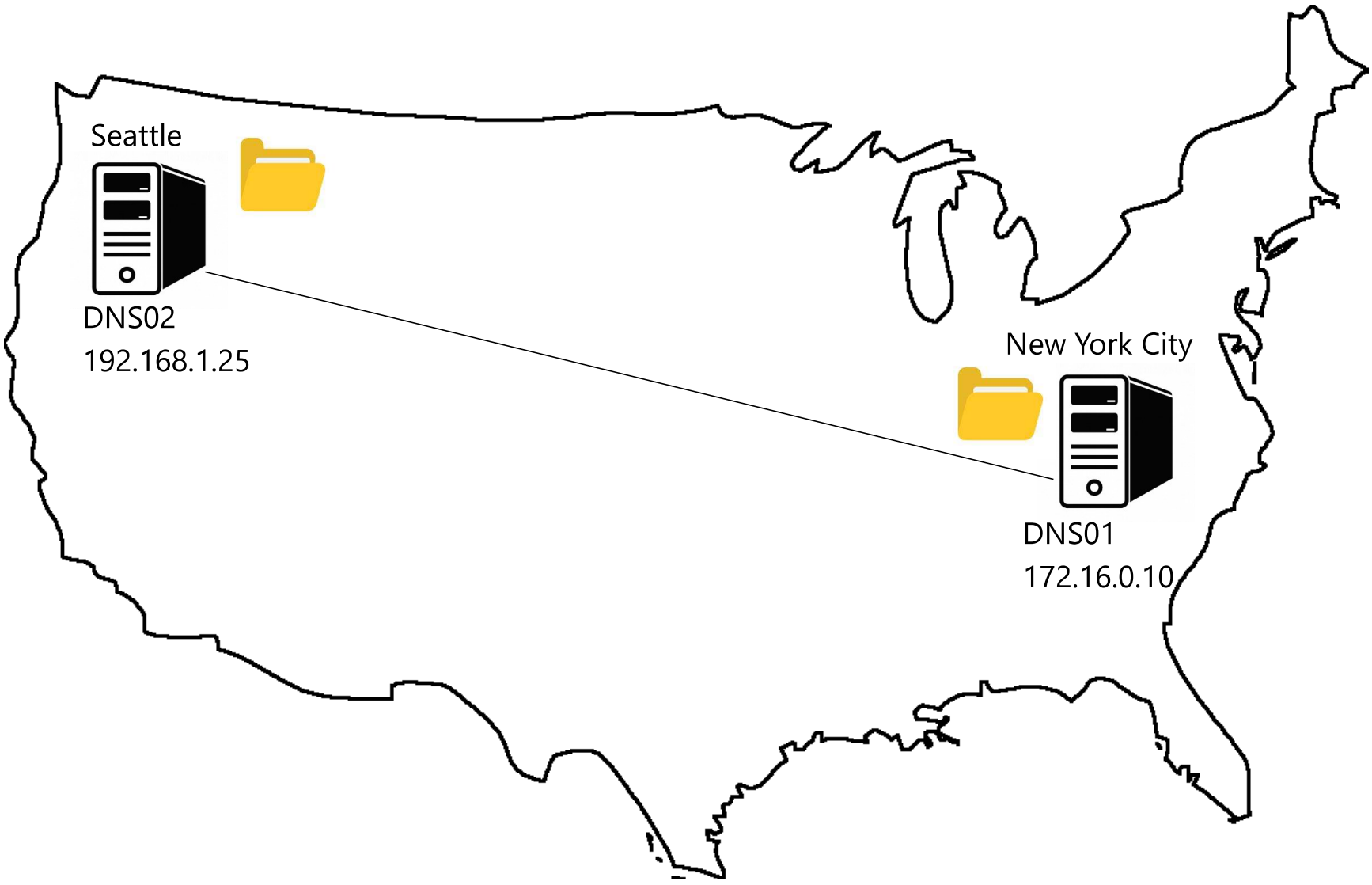
- Read-only copies of primary zones

Stub zones

- contain only the records required to locate and communicate with name servers

Active Directory-integrated zones

- Can only reside on domain controllers
- Replicates with active directory


Seattle
DNS02
192.168.1.25
New York City
DNS01
172.16.0.10

DNS Forwarding

Forwarders:

- Receive DNS requests, and forward requests for zones for which it is not authoritative
- Are common for external name resolution

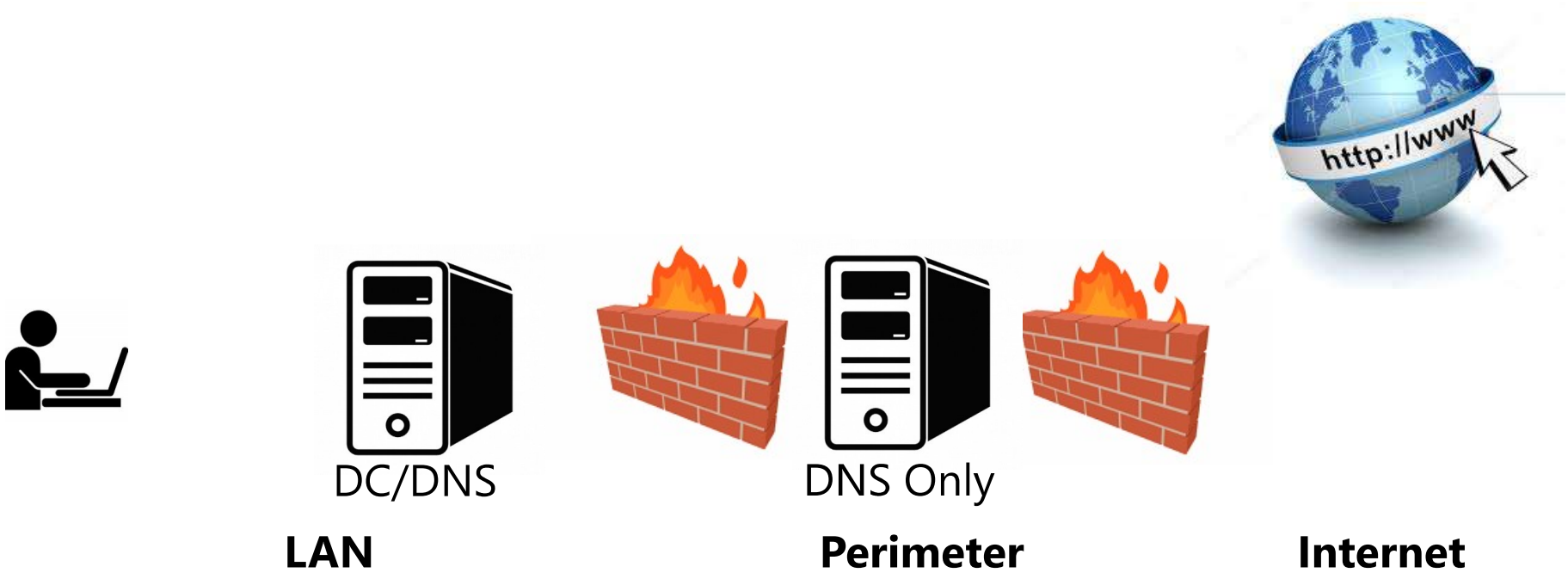
Conditional forwarders:

- Forward requests for a specific domain anme
- Typical between partners and trusted organizations

Stub zones:

- Have a similar role to conditional forwarders
- Are used within the same company
- Requires configuration on both DNS Servers

DNS Forwarding



Module 5:

Managing File Servers and Storage

Module Overview

This module describes how to configure file servers and storage in Windows Server:

- Lessons:
  - Volumes and file systems in Windows Server
  - Implementing sharing in Windows Server
  - Implementing Storage Spaces in Windows Server
  - Implementing Data Deduplication
  - Deploying Distributed File System

Lesson 1 Overview

This lesson describes file systems security in Windows Server:

- Topics:
  - Overview of File Systems in Windows Server
  - Understanding File and Folder level security
  - Managing NTFS permissions
  - Managing Share permissions
  - Managing Permission inheritance
  - File Server Resource Manager (FSRM)
  - Implementing Quotas
  - Implementing File Screens

Overview of file systems in Windows Server

When selecting a file system, consider the differences between FAT, NTFS file system, and ReFS:

- FAT/FAT32 provides:
  - Basic file system
  - No Security
  - exFAT developed for flash drives
- NTFS provides:
  - Auditing
  - Security (permissions and encryption)
  - Compression
- ReFS provides:
  - Backward compatibility support for NTFS
  - Enhanced data verification and error correction
  - Support for larger files, directories, and volumes

File and Folder Level Security

Read

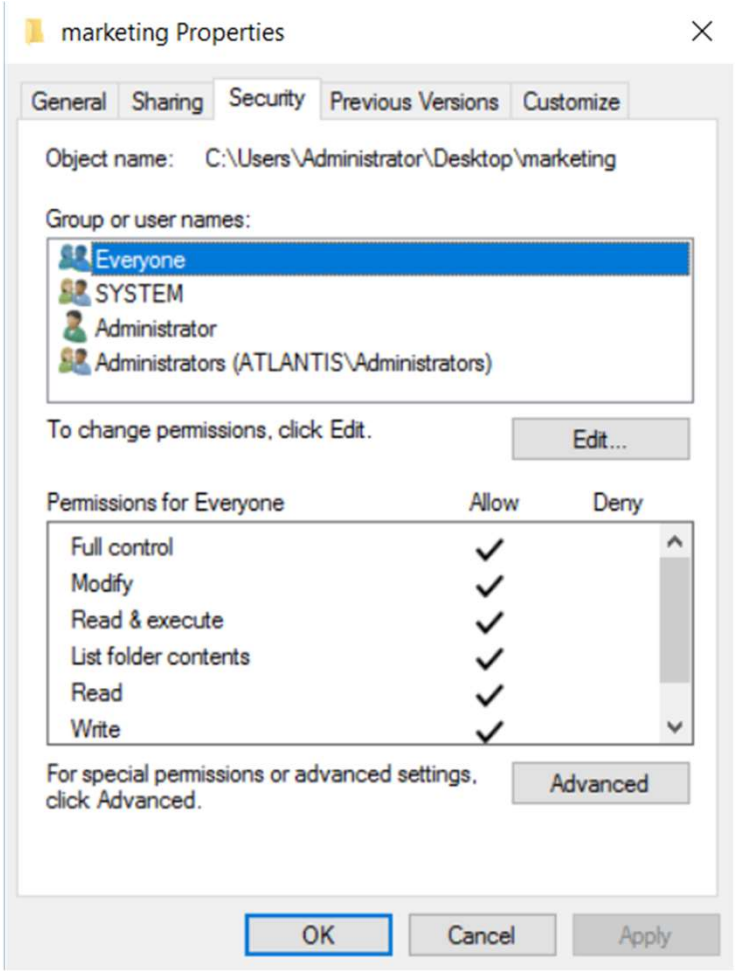
Read and Execute

Write

Modify

Full Control

List Folder Contents



Managing NTFS Permissions

Sales-Reports

Sales Managers

Bob

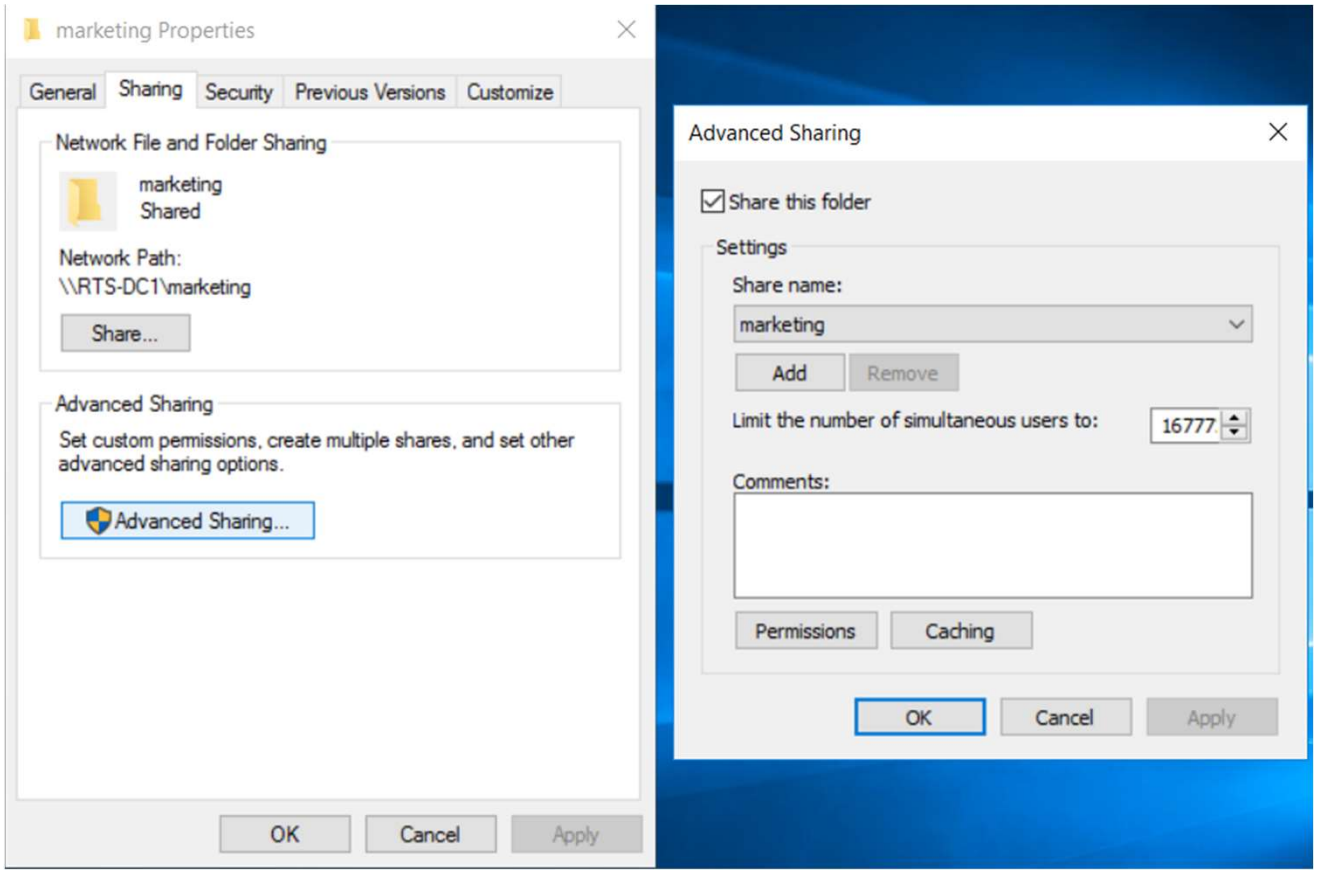
Sales Users

Permissions	**Allow**	**Deny**
Full Control		
Modify	☑	
Read and execute		
List Folder Contents		
Read	☑	
Write		

Managing Shared Folders

Share Permissions:

- Read
- Change
- Full Control



Inheritance

Permissions
Full Control
Modify
Read and execute
List Folder Contents
Read
Write

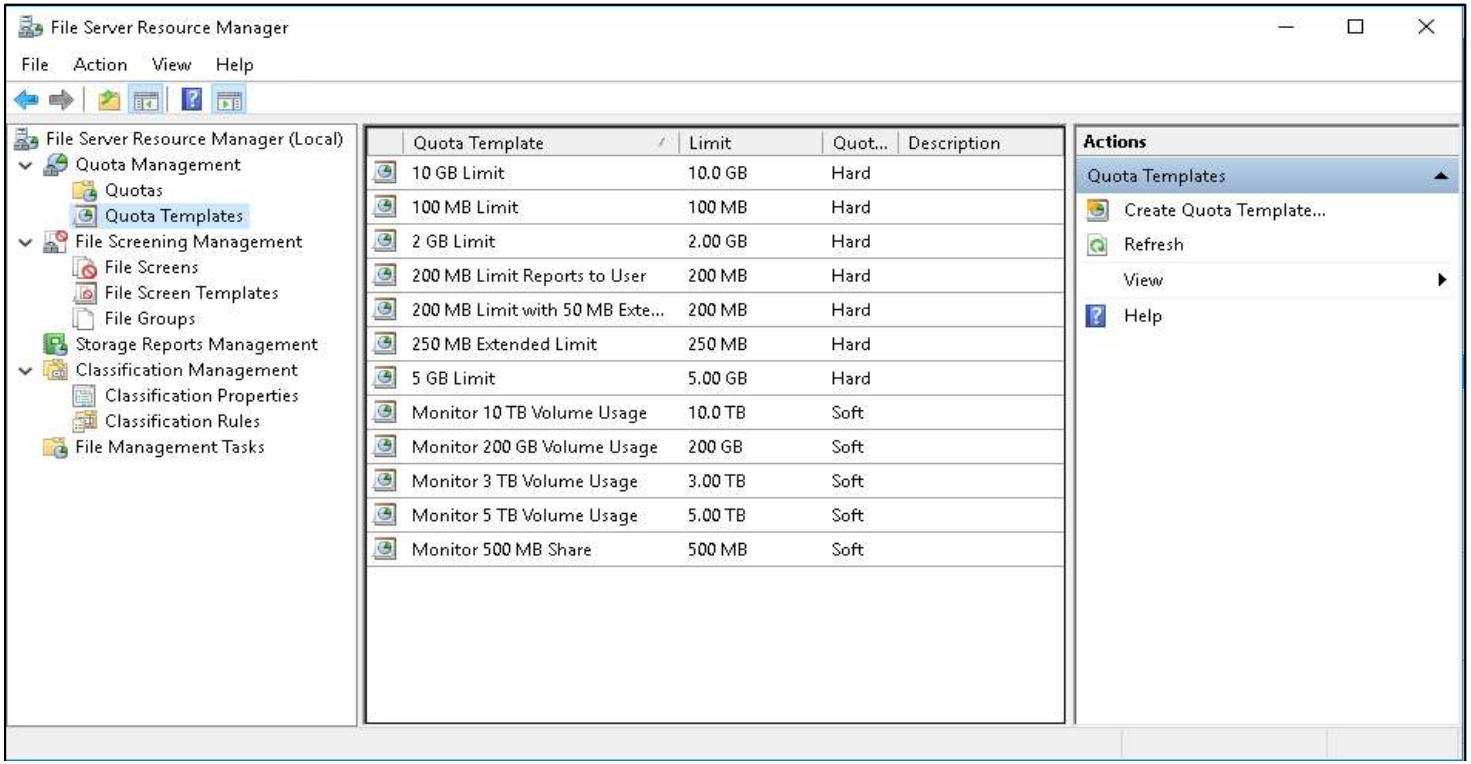
Sales-Reports

Jan-Reports

Permissions
Full Control
Modify
Read and execute
List Folder Contents
Read
Write

Overview of File Server Resource Manager

- Create quotas to monitor and limit the amount of space consumed
- Use a file screen to monitor and block files based on the file extension



Quotas and File Screens

Finance Reports

Quota:

Limit data to 25GB

Do not allow users to exceed quota limit

Send an email to the helpdesk when usage reaches 90% of the quota limit

File Screen:

Block music and video files from being saved

Lesson 2 Overview

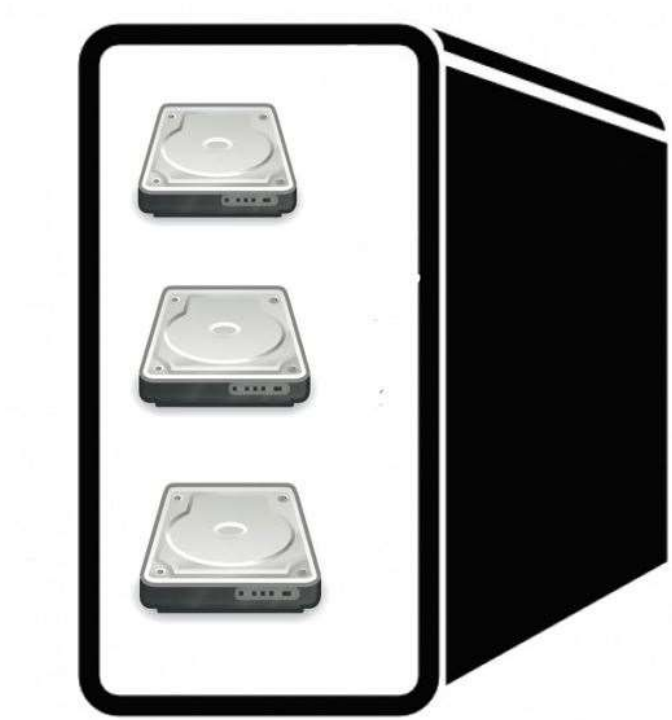
This lesson describes file systems and volumes in Windows Server:

- Topics:
  - Overview of Disk Volumes
  - Basic and Dynamic Disk types
  - RAID

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

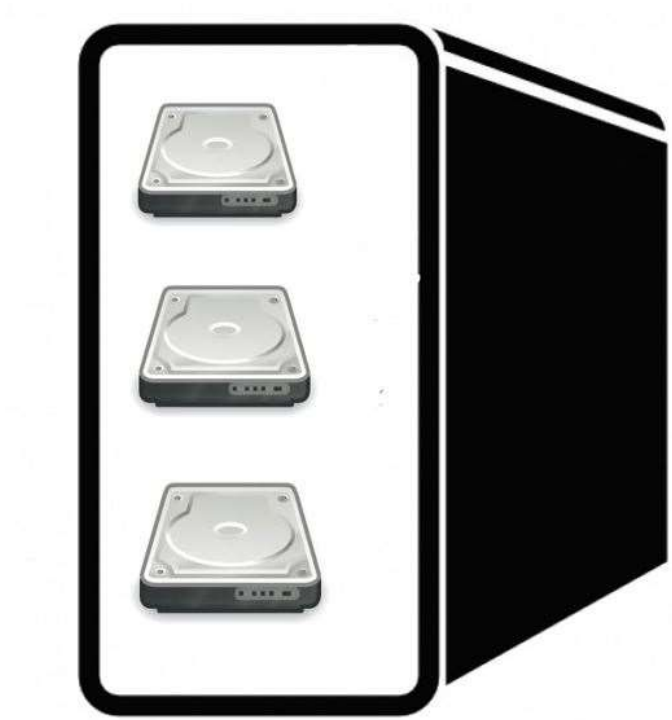
- Basic disk
- Dynamic disk



Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk



Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Overview of disk volumes

When selecting a type of disk for use in Windows Server, you can choose between:

- Basic disk
- Dynamic disk

In Windows Server, if you are using dynamic disks, you can create a number of different types of disk volumes:

- Simple volumes
- Spanned volumes
- Striped volumes
- Mirrored volumes
- RAID-5 volumes

Lesson 3 Overview

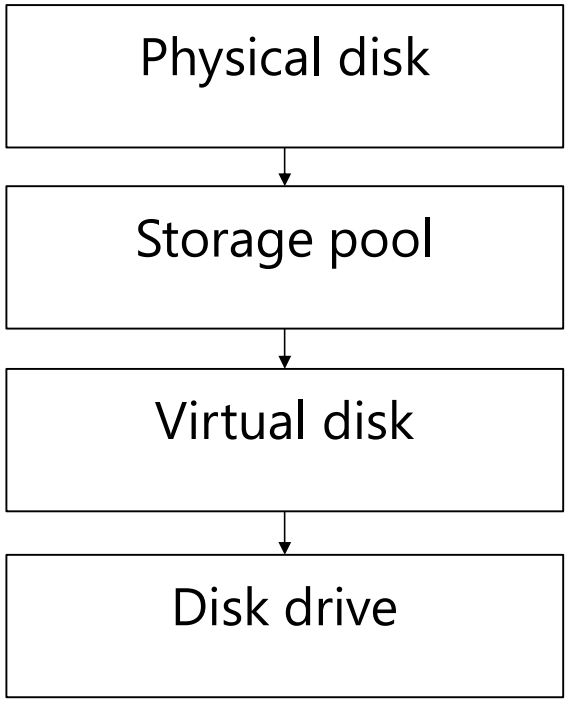
This lesson describes storage spaces in Windows Server:

- Topics:
  - What are Storage Spaces
  - Storage Spaces usage scenarios

What are Storage Spaces?

Use Storage Spaces to:

- Add physical disks of any type and size to a storage pool
- Create highly-available virtual disks from the pool:
  - To create a virtual disk, you need:
    - One or more physical disks
    - A storage pool that includes the disks
    - Virtual disks (or storage spaces) that are created with disks from the storage pool
    - Disk drives that are based on virtual drives



Storage Spaces usage scenarios

Storage Spaces was designed to enable storage administrators to:

- Implement and easily manage scalable, reliable, and inexpensive storage
- Use inexpensive storage with or without external storage
- Combine multiple drives into storage pools that administrators can manage as a single entity
- Implement different types of storage in the same pool
- Grow storage pools as required
- Provision storage as required from existing storage pools
- Designate specific drives as hot spares

Lesson 4: Overview

This lesson describes how to implement the Data Deduplication feature:

- Topics:
  - Data Deduplication components
  - Data Deduplication process
  - Deploying Data Deduplication
  - Backup and restore considerations with Data Deduplication

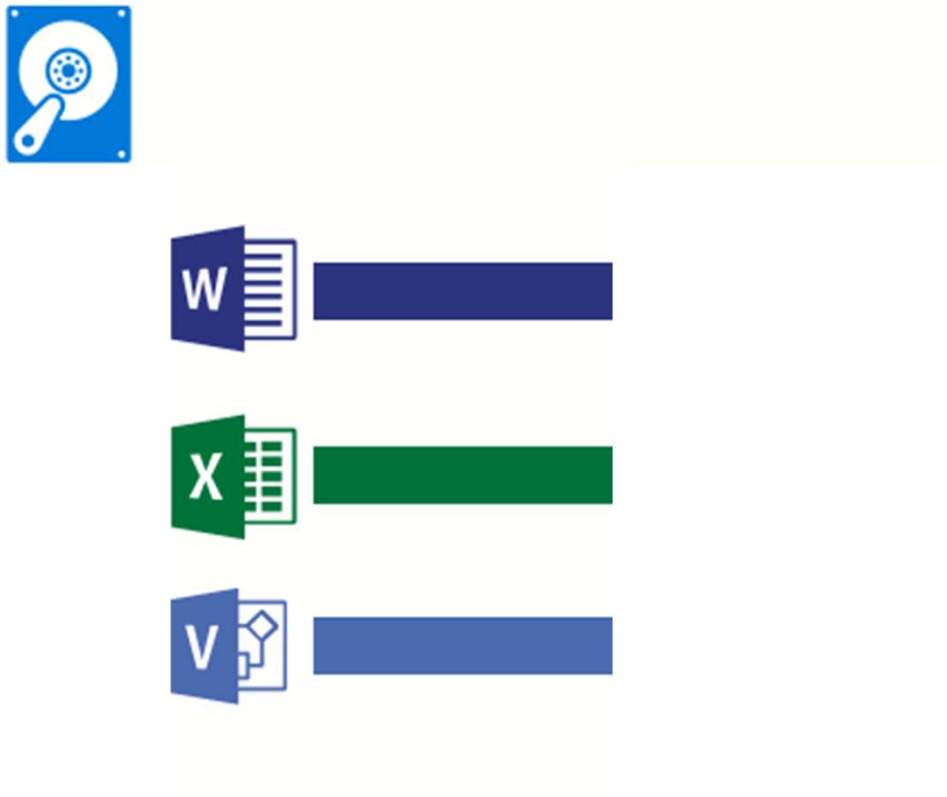
Data Deduplication

- **Data Deduplication**, often called **Dedup** for short, is a feature that can help reduce the impact of redundant data on storage costs.
- When enabled, Data Deduplication optimizes free space on a volume by examining the data on the volume by looking for duplicated portions on the volume.
- Duplicated portions of the volume's dataset are stored once and are compressed for additional savings.

Scenario	Content	Typical space savings
User documents	Office documents, photos, music, videos, etc.	30-50%
Deployment shares	Software binaries, cab files, symbols, etc.	70-80%
Virtualization libraries	ISOs, virtual hard disk files, etc.	80-95%
General file share	All the above	50-60%

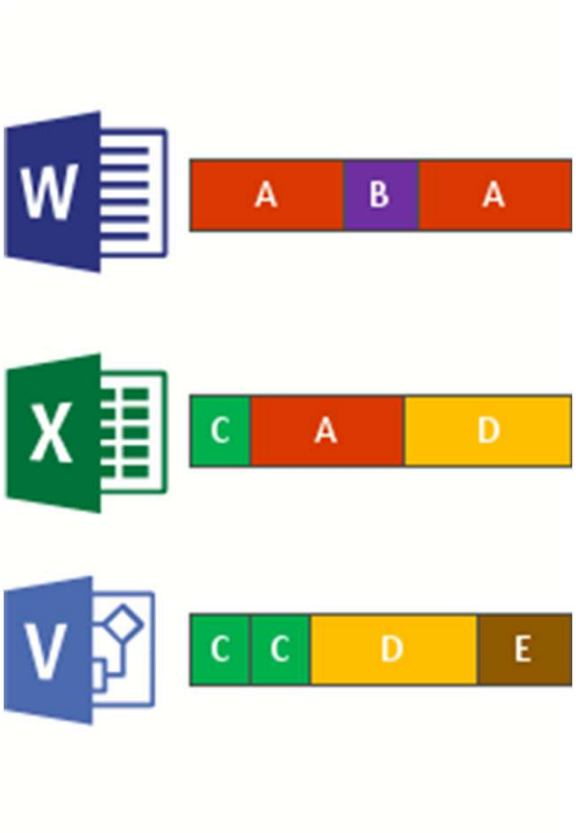
Data Deduplication

1. Scan the file system for files meeting the optimization policy



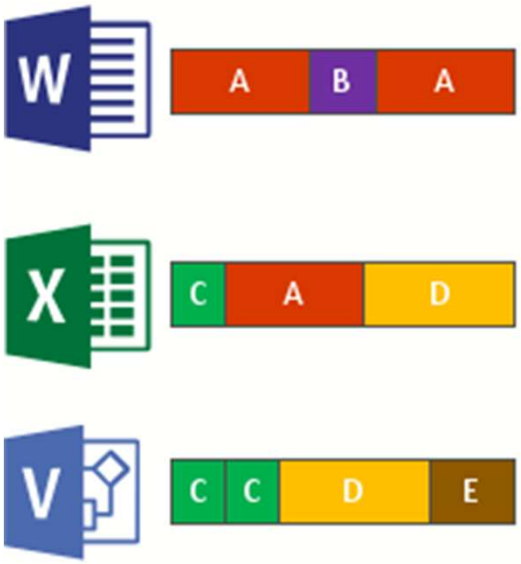
Data Deduplication

2. Break files into chunks



Data Deduplication

3. Identify unique chunks
4. Place chunks in the chunk store and compress



Data Deduplication

5. Replace the original file stream of now optimized files with a reparse point to the chunk store

Deploy Data Deduplication

Prior to installing and configuring Data Deduplication in your environment, plan your deployment using the following steps:

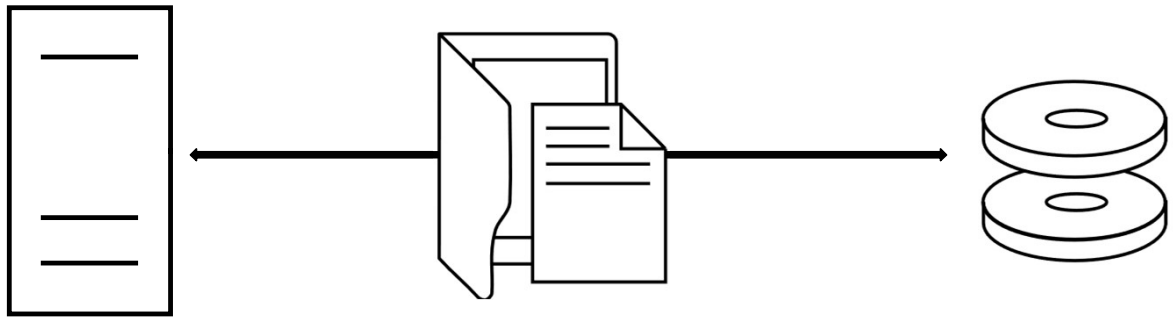
1. Determine target deployments (the drive to which you want to deploy dedpup)
2. Determine which volumes are candidates for deduplication
3. Evaluate savings with the **Deduplication Evaluation Tool**
4. Plan the rollout and deduplication policies

Deploy Data Deduplication

After completing your planning, deploy Data Deduplication to a server in your environment by performing the following steps:

1. Install Data Deduplication components on the server
2. Enable Data Deduplication
3. Configure Data Deduplication jobs
4. Configure Data Deduplication schedules

Backup and restore considerations with Data Deduplication



One of the benefits of using Data Deduplication is that backup and restore operations typically are faster

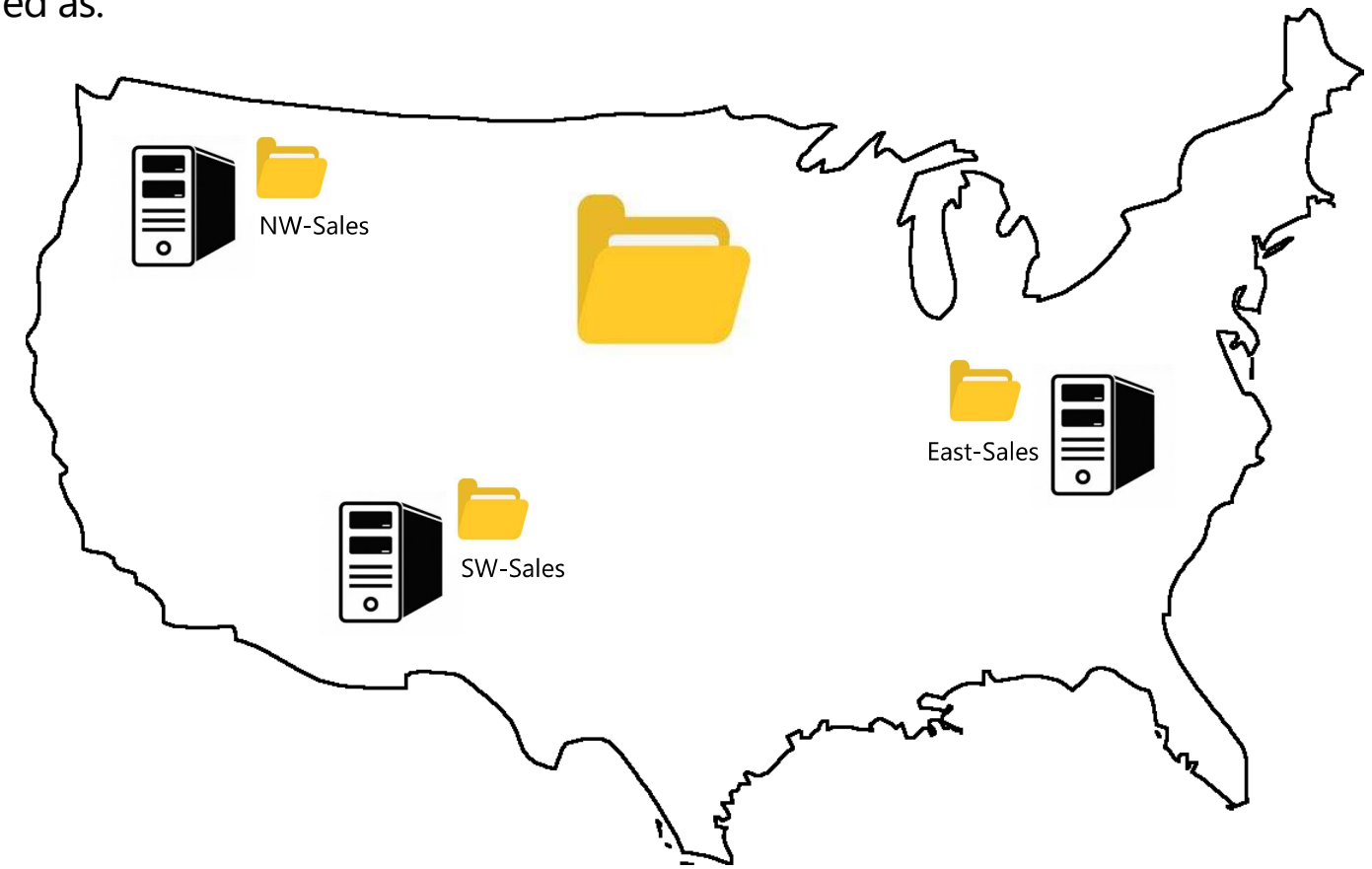
Lesson 5: Overview

This lesson describes how to manage DFS databases

- Topics:
  - Understanding DFS namespace
  - Understanding DFS Replication
  - Implement DFS namespace and replication solutions

DFS namespaces

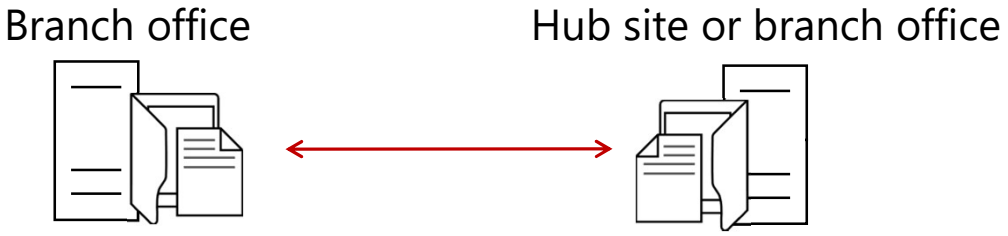
- DFS namespaces can be configured as:
  - Domain-based namespaces
  - Standalone namespaces



DFS Replication

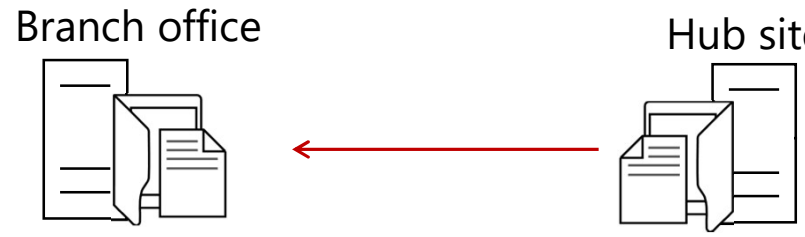
Three DFS scenarios:

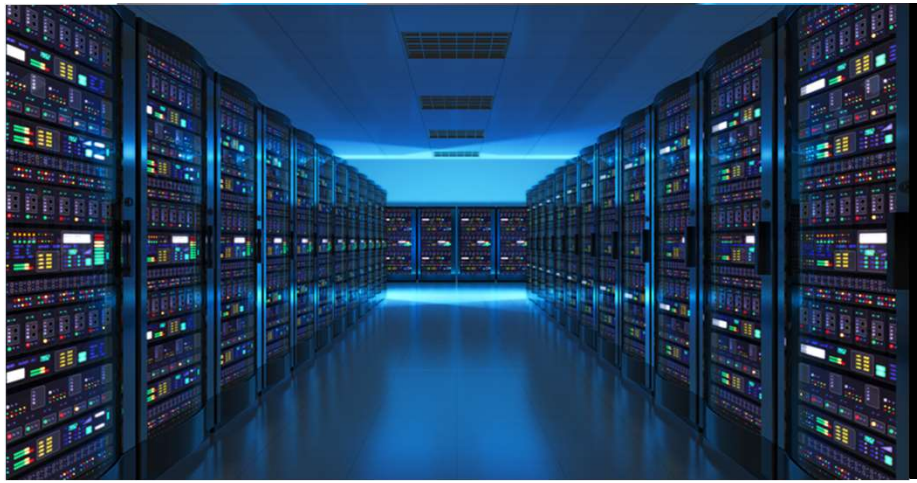
Sharing files across branch offices



Data collection

Data distribution





Module 6:

Implementing Hyper-V Virtualization

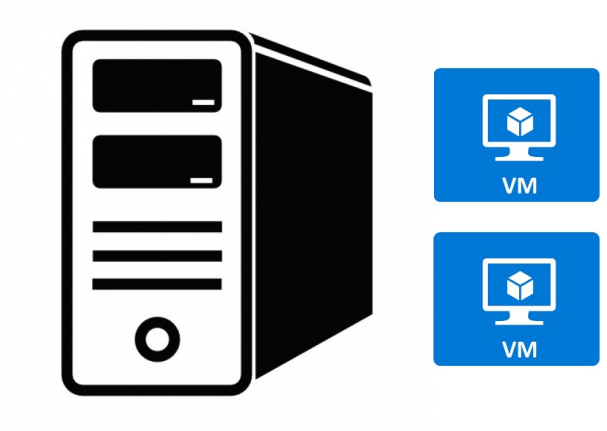
Lesson 1 Overview

This lesson provides an overview of Hyper-V :

- Topics:
  - Understanding Hyper-V
  - Hyper-V manager
  - Best practices for Hyper-V configurations

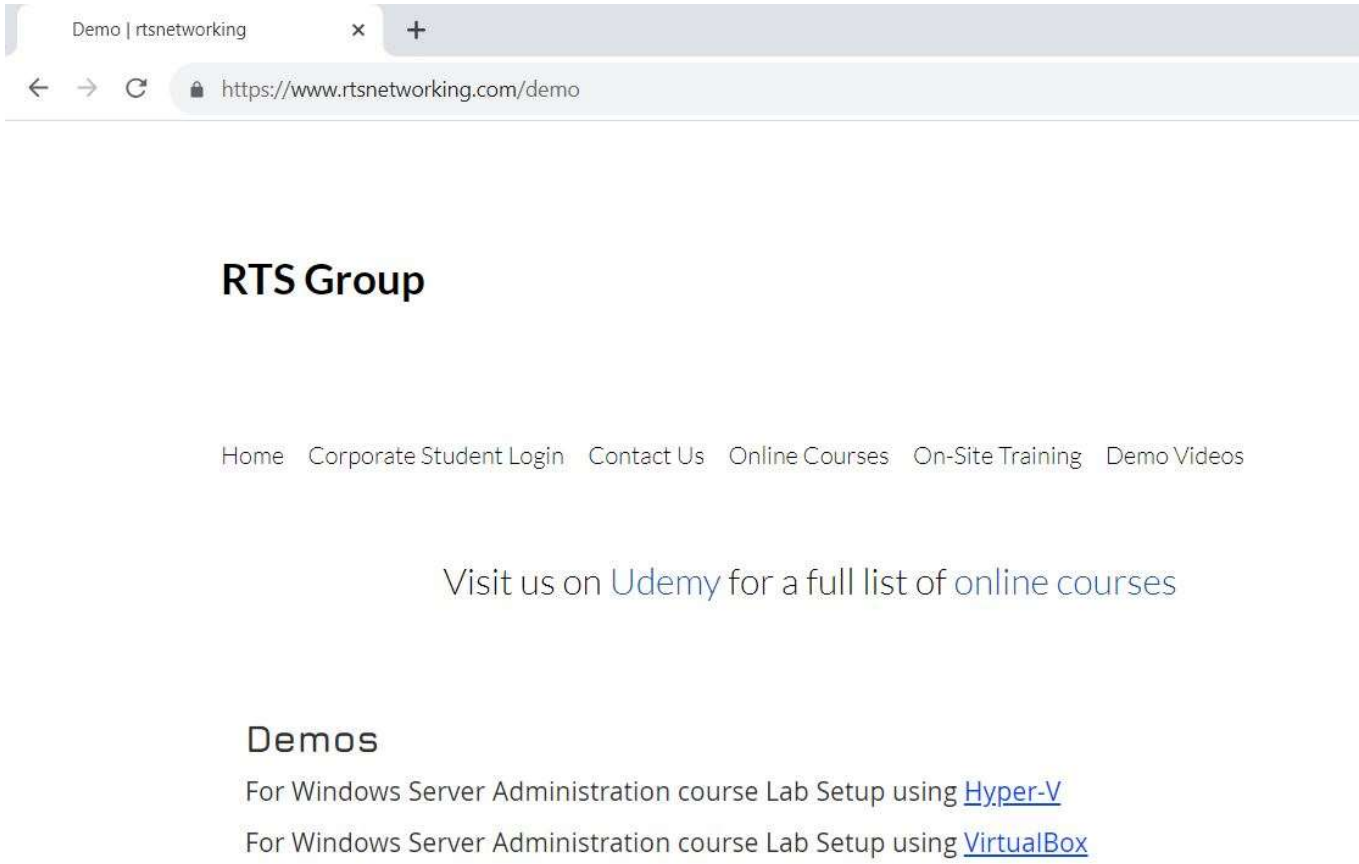
Overview of Hyper-V

- Hyper-V is a hardware virtualization server role available for Windows Server
- Provides a software layer known as the *Hypervisor*, used to control access to physical hardware
- Supports many types of guest operating systems including:
  - All supported Windows versions
  - Linux
- General Hyper-V features can be grouped as follows:
  - Management and connectivity
  - Portability
  - Disaster recovery and backup
  - Security
  - Optimization



Installing Hyper-V

https://RTSnetworking.com/demo



Overview of Hyper-V

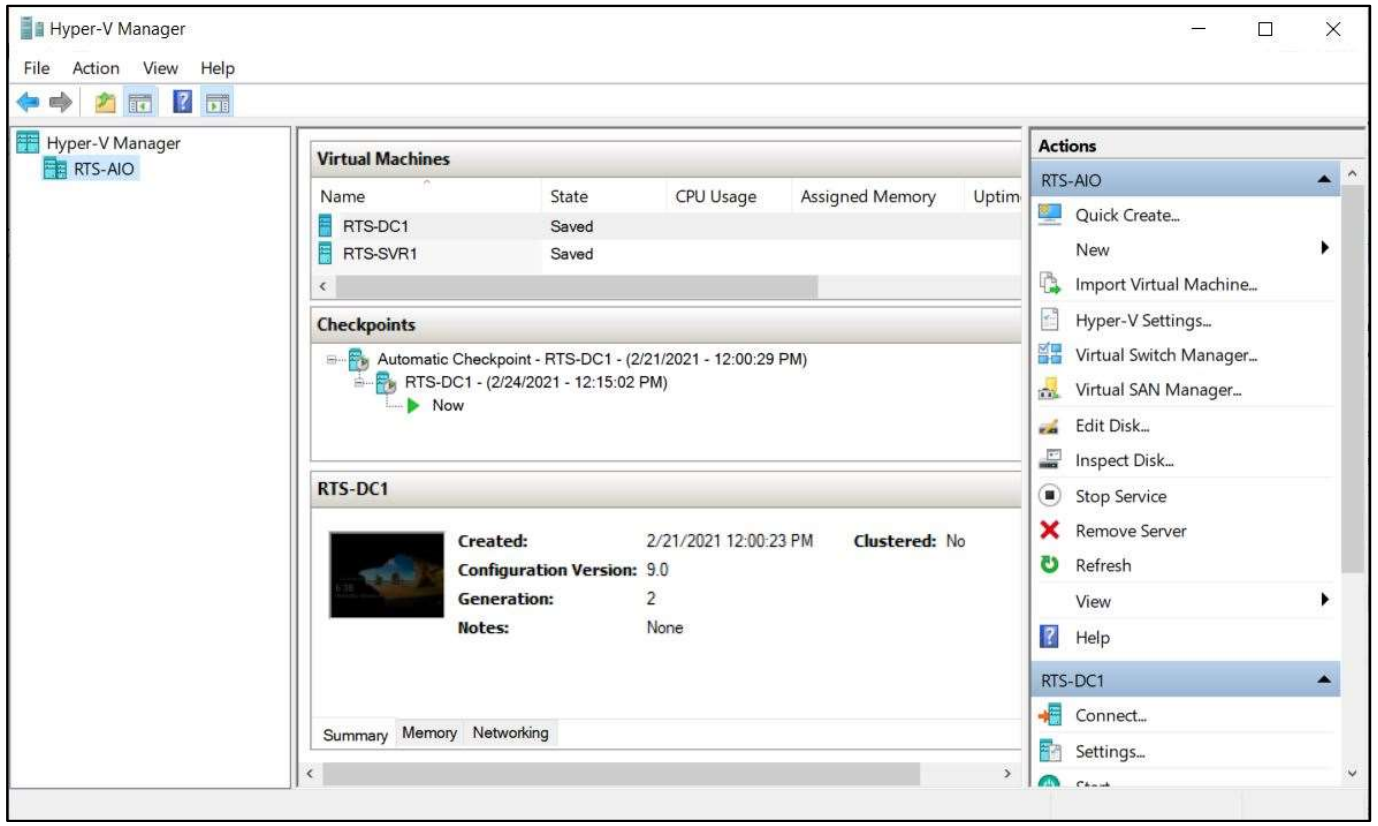
- System requirements for installing the Hyper-V server role include:
  - A 64-bit processor
  - Sufficient memory
  - Intel Virtualization Technology (Intel VT) or Advanced Micro Dynamics (AMD) Virtualization (AMD-V) enabled

  To verify you meet the requirements, run **MSINFO32**

- Methods to install the Hyper-V server role include:
  - Server Manager
  - **Install-WindowsFeature** PowerShell cmdlet

Overview of Hyper-V Manager

- A graphical user interface used to manage both local and remote Hyper-V host machines
- Other management tools include:
  - Windows PowerShell
  - Windows Admin Center



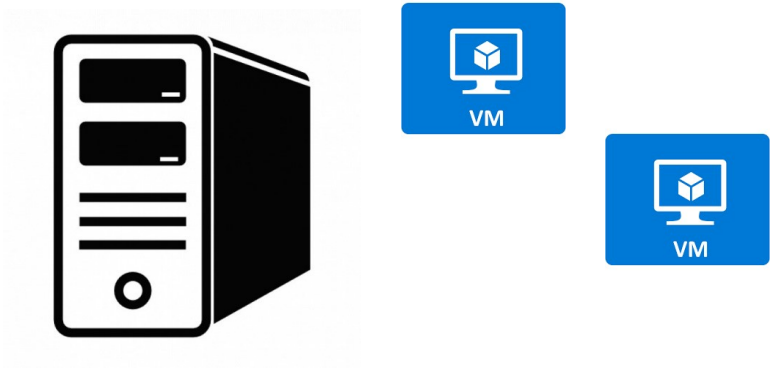
Best practices for configuring Hyper-V hosts

- Consider the following when provisioning Windows Server as a Hyper-V host:
  - Provision the host with adequate hardware
  - Deploy virtual machines on separate disks, solid state drives
  - Do not collocate other server roles
  - Manage Hyper-V remotely
  - Run Hyper-V by using a Server Core configuration

Overview of nested virtualization

- Provides the ability to install the Hyper-V role within a guest virtual machine
- Requirements:
  - Both the Hyper-V host and the guest virtual machine must be Windows Server 2016 or later
  - Sufficient amount of static RAM

Set-VMProcessor -VMName <*VMName*> -ExposeVirtualizationExtensions $true



Lesson 2 Overview

This lesson describes configuring virtual machines:

- Topics:
  - Configuring VMs
  - VM Settings
  - Virtual Hard Disks
  - Virtual Networking
  - Managing Checkpoints

VM generation versions

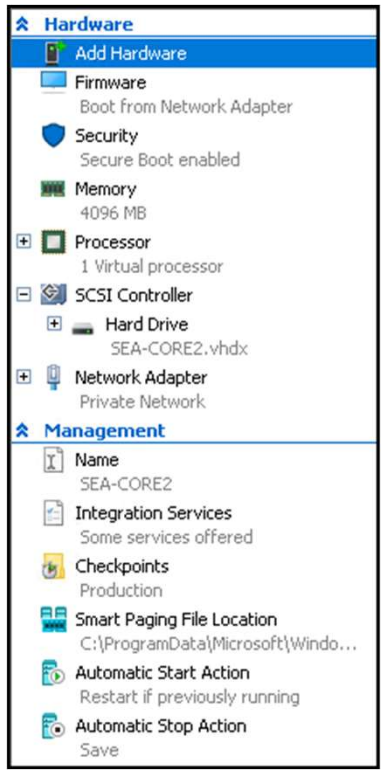
- Generation 1 VMs:
  - Support 32 and 64-bit operating systems
  - Only support boot volumes a maximum of 2 TB
  - Supports legacy BIOS
- Generation 2 VMs:
  - Support only 64-bit operating systems
  - Support secure boot and shielded VMs
  - Support boot volumes a maximum of 64 TB
  - Supports Unified Extensible Firmware Interface (UEFI)

VM settings

- VM settings are grouped into two main areas:
  - Hardware
  - Management
- Available hardware components depend on the generation version of the VM

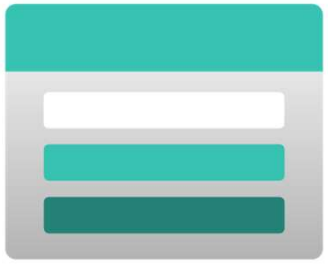
Generation 1 settings

Generation 2 settings



Storage options in Hyper-V

- Consider the following factors when planning storage for virtual hard disks:
  - High-performance connection to storage
  - Redundant storage
  - High-performance storage
  - Adequate growth space



Virtual hard disk formats and types

- Virtual hard disk formats include:
  - VHD
    - Up to 2040 GB in size
    - Typically used to support older Hyper-V versions
  - VHDX:
    - Up to 64 TB in size
    - Recovery from corruption issues
    - Supports larger block size resulting in increased performance
- Use the **Edit Virtual Hard Disk Wizard** to convert between hard disk formats
- Various tools can be used to create and mange virtual hard disks:
  - Hyper-V Manager
  - Disk Management/Diskpart
  - PowerShell (New-VHD)
  - Windows Admin Center

Virtual hard disk formats and types

Type of disc	Description
Fixed	Allocates all of the hard disk space immediately
Dynamic	The disk only uses the amount of space that needs to be allocated, and it grows as necessary
Differencing	Associated with another virtual hard disk in a parent-child configuration. Any changes made to the differencing disk does not affect the parent disk.
Pass through	Allows the virtual machine to connect directly to an Internet Small Computer Systems Interface (iSCSI) (logical unit number) LUN or a physical disk attached on the host machine

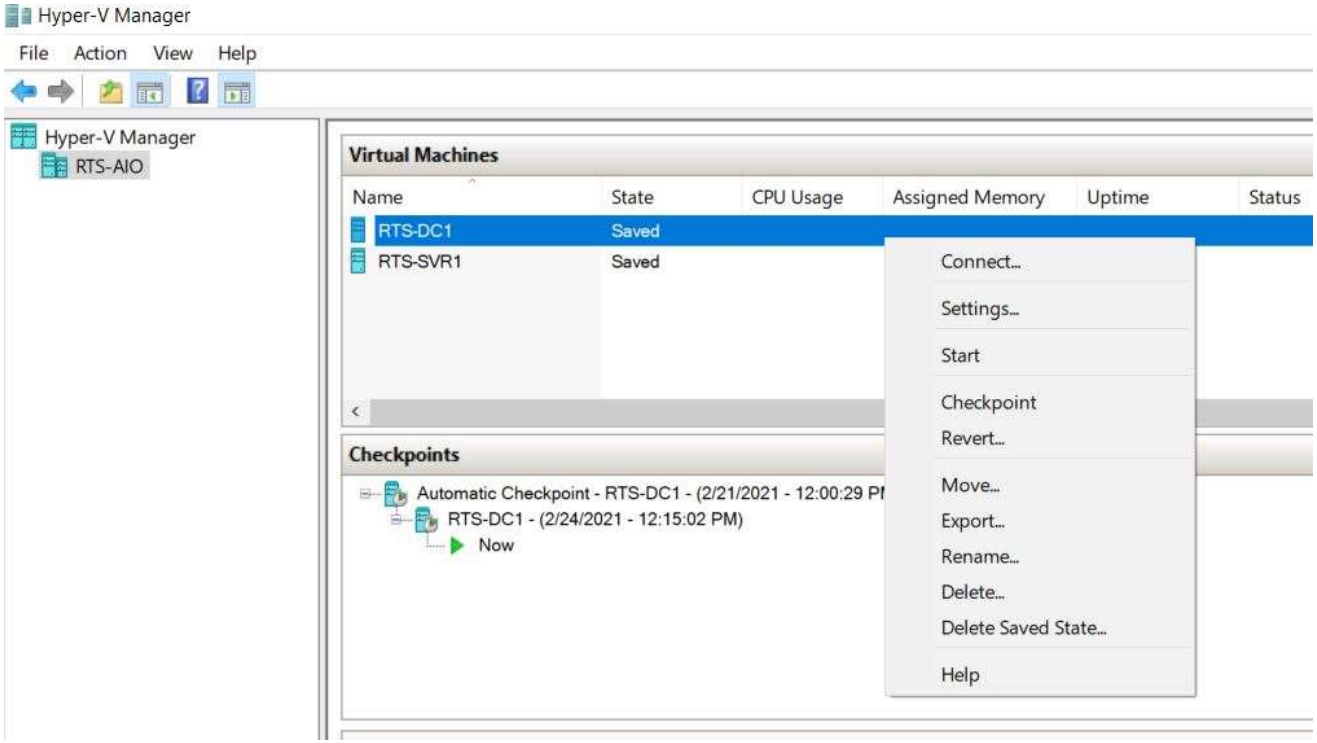
Overview of Hyper-V networking

- Hyper-V supports three types of virtual switches:

Virtual switch type	Description
External	Provides external access outside of the host machine by mapping to a network adapter in the host, which is used for communication.
Internal	Used to communicate between the virtual machines on a host server and to communicate between the virtual machines and the host itself
Private	Used to only communicate between virtual machines on a Hyper-V host, but does not allow communication with the host itself

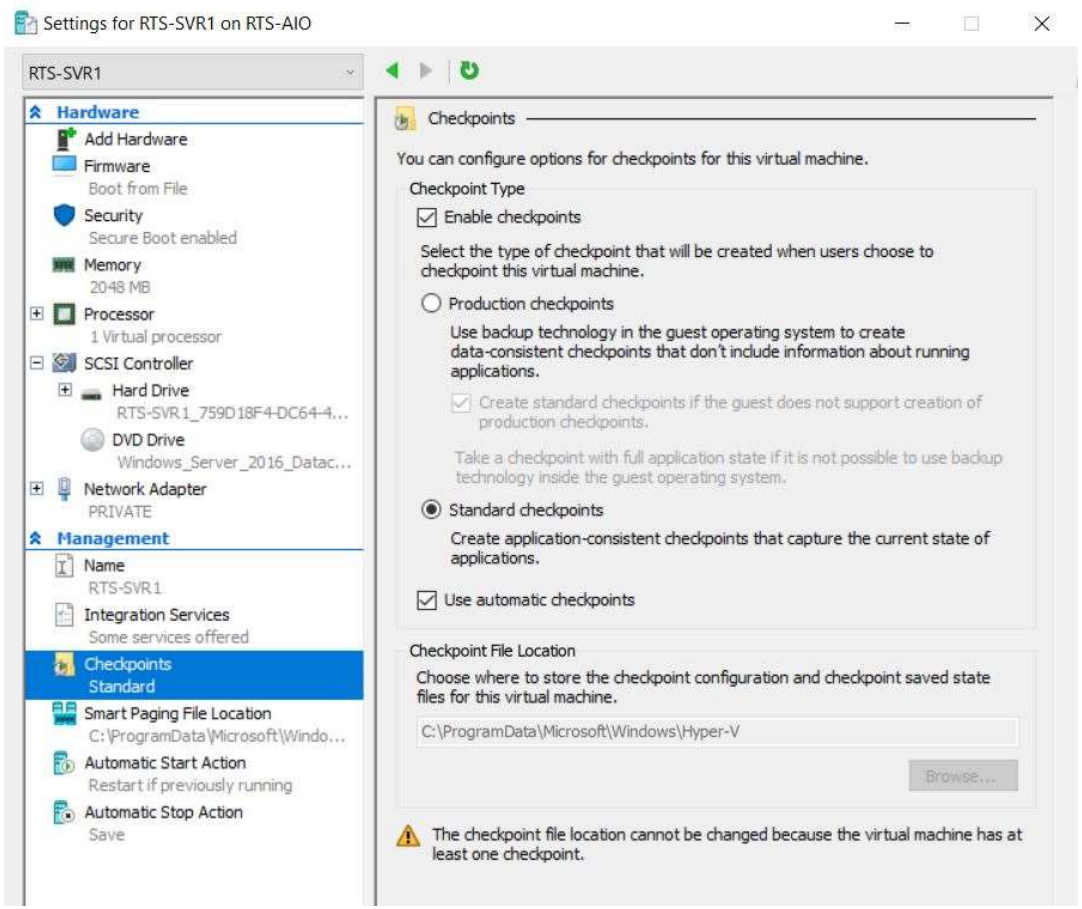
Manage VM states and checkpoints

- A VM can be in one of the following states:
  - Off
  - Starting
  - Running
  - Paused
  - Saved



Manage VM states and checkpoints

- Checkpoints:
  - Allows you to take a snapshot of a virtual machine at a specific point in time
  - Two types of checkpoints
    - Production checkpoints
    - Standard checkpoints
  - Maximum of 50 checkpoints per virtual machine allowed



Module 7:

Implementing Windows Print Server

Lesson 1 overview

In this lesson, you'll learn about Windows Print Server management, security, and performance capabilities and configurations.

Topics:

- Windows Print Server
- How a Windows Print Server works
- Windows Print Server Best Practices
- Type 3 vs Type 4 Printer
- Print Permissions
- Print Pooling
- Print Priority

Windows Print Server

A Windows print server is a computer that manages printers and makes them available to print clients on a network. It acts as a central point for managing print jobs and printer settings.

Benefits of using a Windows print server

There are several benefits to using a Windows print server, including:

•Centralized management: A print server provides a central location for managing all of the printers on a network. This makes it easier to install and configure printers, update printer drivers, and troubleshoot printing problems.

•Improved performance: A print server can improve the performance of printing by spooling print jobs and sending them to printers in an efficient manner.

•Security: A print server can help to improve the security of printing by restricting access to printers and printer settings.

•Scalability: A print server can be scaled to support a large number of printers and users.

How a Windows Print Server works

When a user sends a print job to a print server, the print server spools the print job and then sends it to the appropriate printer. The print server also monitors the status of printers and print jobs, and it can notify users if there are any problems.

Deploying a Windows print server

To deploy a Windows print server, you will need to:

1. Install the Print Server role on a Windows server.
2. Add printers to the print server.
3. Configure printer settings and permissions.
4. Point print clients to the print server.

Windows Print Server Best Practices

Best practices for using a Windows print server

•Use a dedicated print server: If possible, use a dedicated server for printing. This will help to improve the performance and reliability of printing.

•Keep printer drivers up to date: Make sure to keep the printer drivers on the print server and print clients up to date. This will help to prevent printing problems.

•Configure printer permissions carefully: Carefully configure printer permissions to restrict access to printers and printer settings. This will help to improve the security of printing.

•Monitor printer usage: Monitor printer usage to identify printers that are not being used frequently and to identify printers that are experiencing a high volume of print jobs. This information can be used to make informed decisions about printer placement and configuration.

Type 3 vs Type 4 Printer

Feature	Type 3	Type 4
Architecture	Older	Newer
Provider	Printer manufacturer	Microsoft
Distribution	Typically downloaded from the printer manufacturer's website	Typically bundled with the operating system or downloaded from Windows Update
Installation	Requires administrative rights	Can be installed by standard users
Features	Typically supports all of the features of the printer	May not support all of the features of the printer
Compatibility	Compatible with all versions of Windows	Compatible with Windows 8 and later

Print Permissions

On Windows systems, there are three levels of print permissions:

•**Print**: This permission allows users to connect to the printer and print, pause, resume, start, and cancel their own documents.

•**Manage Documents**: This permission allows users to control job settings for all documents and to pause, restart, and delete all documents.

•**Manage Printer**: This permission allows users to pause and restart the printer, change spooler settings, share a printer, adjust printer permissions, and change printer properties.

By default, all users on a network have the Print permission. However, system administrators can change these permissions to restrict access to certain printers or to allow users to perform only certain printing tasks.

Print Pooling

Requirements:

- Same print Driver
- Location

Print Priority

Sales Users

Sales Managers

Module 8:

Disaster Recovery on Windows Server 2022

Lesson 1 overview

In this lesson, you'll learn about Windows Server backup and restore capabilities and the integration with Azure Backup

Topics:

- Overview of Windows Server Backup
- Implement backup and restore
- Back up and restore Hyper-V VMs
- Overview of Azure Backup

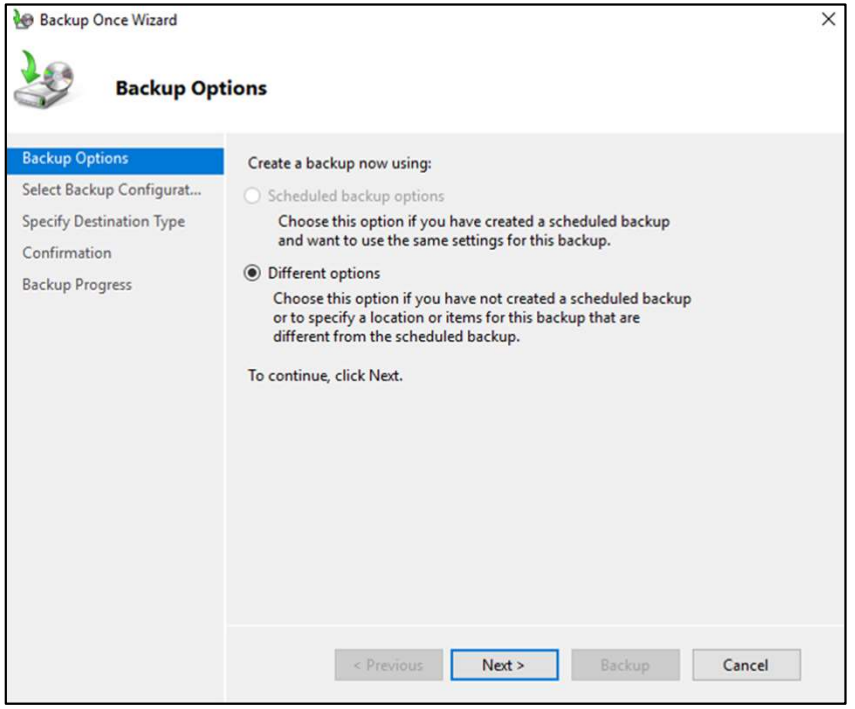
Overview of Windows Server Backup

Windows Server Backup provides you with the ability to perform backup and recovery in a Windows Server environment

By using Windows Server Backup you can backup:

- A full server (all volumes), or just selected volumes
- Individual files and folders
- System state
- Individual virtual machines on a Hyper-V host

WBAdmin is a command-line utility built into Windows Server

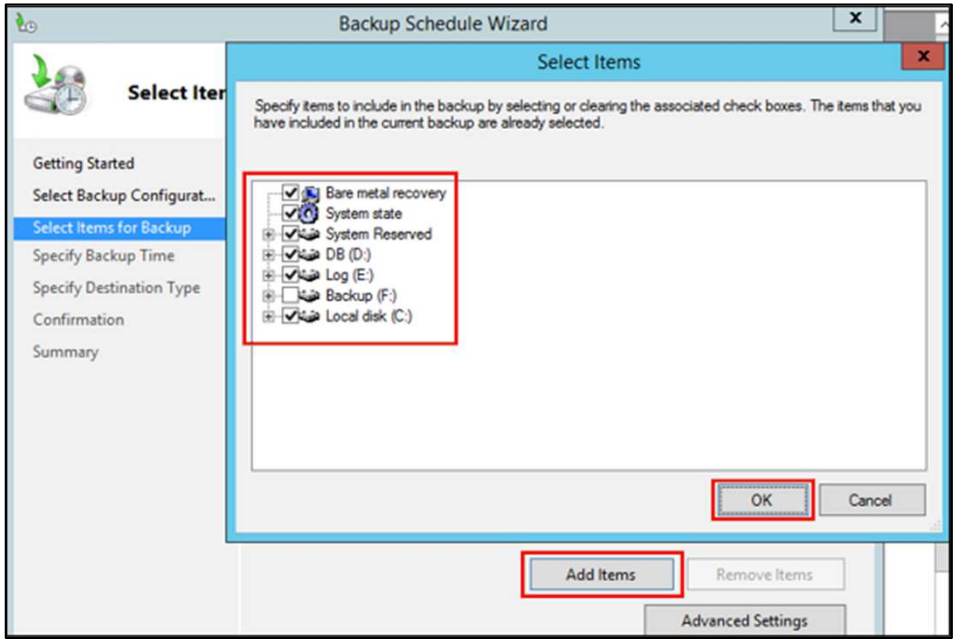


Implement backup and restore

Depending on what you need to backup, the procedures and options in Windows Server Backup might vary

Some of the most common backup procedures that you should consider include:

- Backing up file servers and web servers
- Backing up AD DS
- Backing up Microsoft Exchange Server



Back up and restore Hyper-V VMs

You can use the following methods to back up VMs:

- Backup the VM from the host
- Backup the VM's VHDs
- Backup inside the VM

You can perform online backups that do not incur VM downtime, if you meet the following conditions:

- The VM being backed up has integration services installed and enabled
- Each disk that the VM uses is running NTFS file system basic disks
- The VSS is enabled on all volumes within the VM

Overview of Azure Backup

Azure Backup is a subscription service that you can use to provide off-site protection against critical data loss caused by disasters

Azure Backup replaces or extends your existing on-premises or off-site backup solution

Some of the most important features in Azure Backup include:

- Automatic storage management
- Unlimited scaling
- Data encryption
- Offload on-premises backup
- Back up Azure VMs

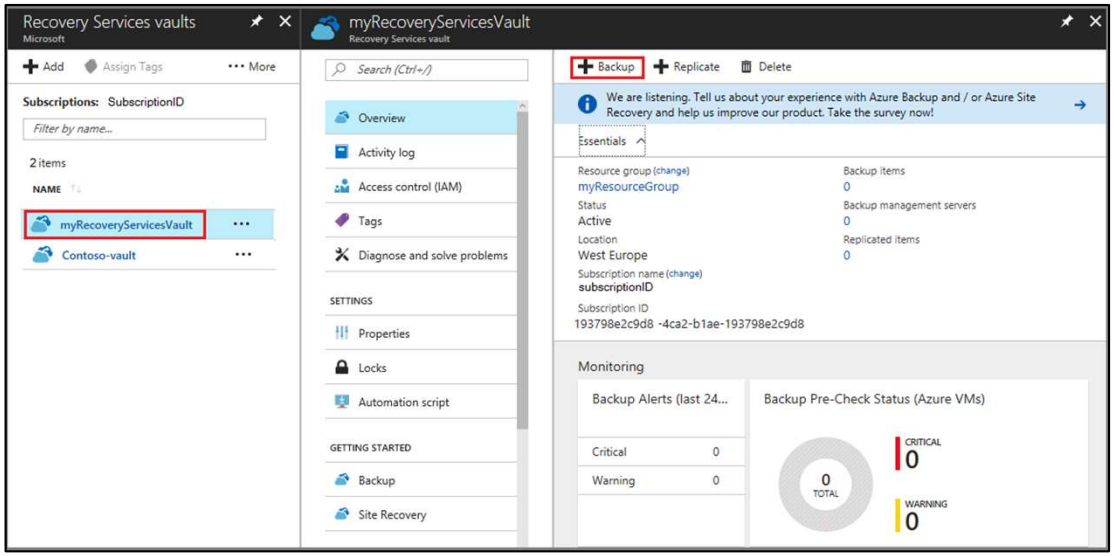
Implement backup and restore with Azure Backup

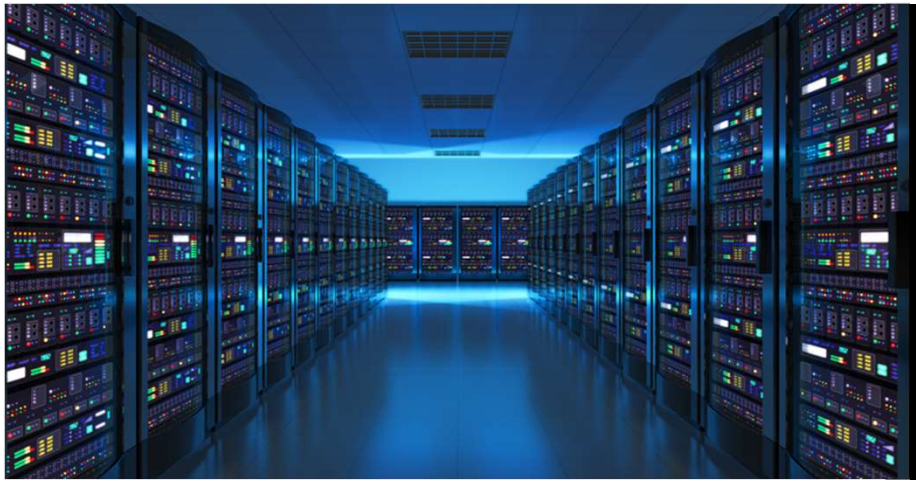
To use Azure Backup, you need to install a backup agent on your local servers, and you need to configure an Azure Recovery Services vault

You can use Recovery Services vaults to hold backup data for various Azure services such as VMs (Linux or Windows) and Azure SQL databases

Within an Azure subscription, you can create up to 25 Recovery Services vaults per region

Azure Backup for files and folders relies on the Azure Recovery Services agent to be installed on the Windows client or server





Module 9:

Implementing Windows Server Update Services on Windows Server 2022

Lesson 1 overview

This lesson describes Windows Server Update Service (WSUS).
It provides infrastructure to download, test, and approve updates which help block attacks

- Topics:
  - Overview of Windows Update
  - What is WSUS?
  - WSUS Requirements
  - WSUS Deployment Options
  - WSUS Administration Console
  - Managing Updates
  - Configuring Clients

Overview of Windows Update

- Windows Update is a Microsoft service that provides updates for Microsoft software
- Orchestrator on devices scans for and downloads updates
- Clients and servers can be configured to get updates from the Windows Update Services server

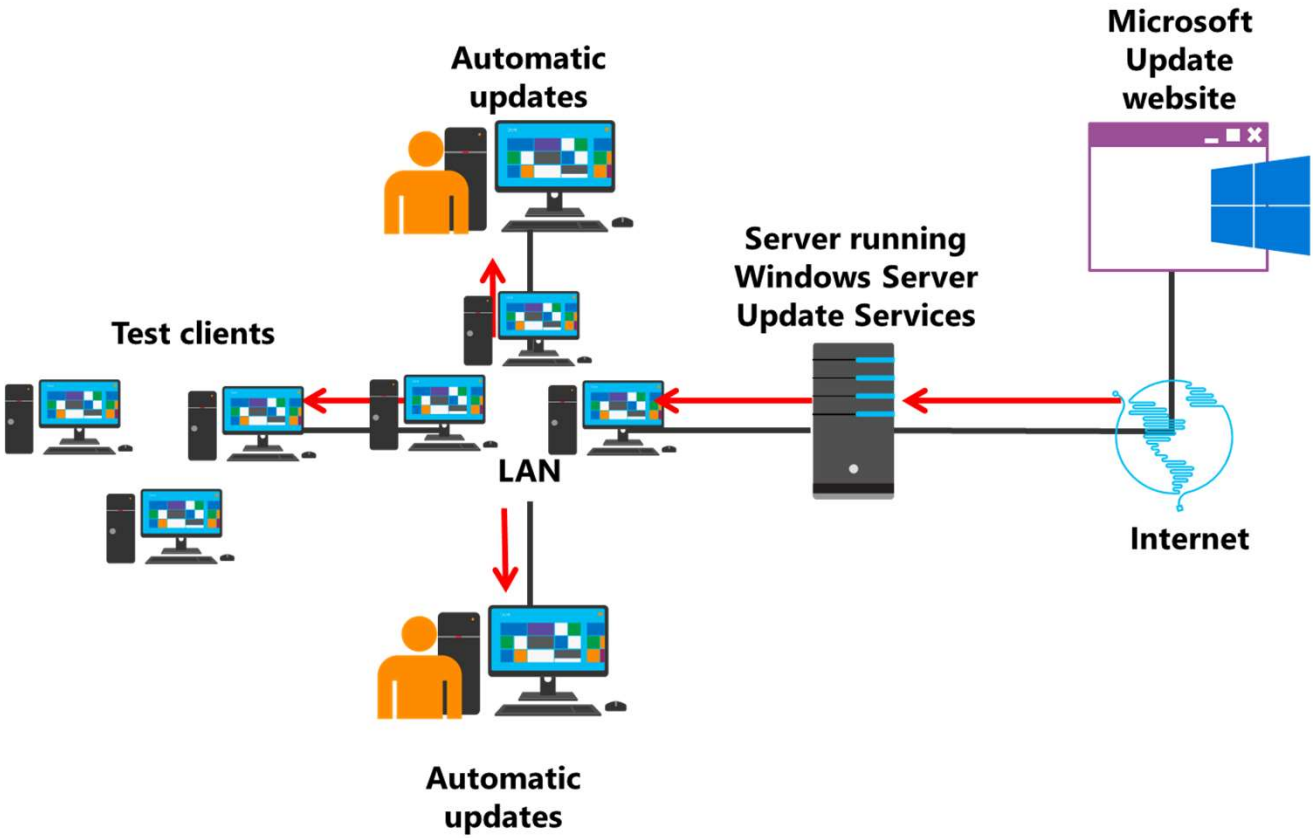
What is WSUS?

WSUS provides an infrastructure for managing updates for Windows devices

WSUS allows you to:

- Choose the updates you want to download
- Test updates before broad deployment
- Choose which devices get updates and when they receive them
- Track status of updates

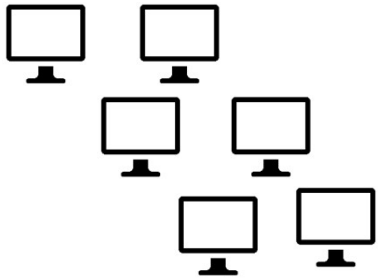
What is WSUS?


Automatic updates
Microsoft Update website
Server running Windows Server Update Services
Test clients
LAN
Internet
Automatic updates

WSUS Requirements

Prerequisites:

- 1.4 gigahertz (GHz) or faster x64 processor
- 2 gigabytes (GB) of random-access memory (RAM) or greater (above that needed for other roles)
- 10 GB or greater
- 100 megabits per second (Mbps) or greater network adapter
- .NET Framework 4.0
- Microsoft Report Viewer Runtime 2012
- Windows Internal Database or Microsoft SQL Server



Microsoft Update

WSUS server deployment options

WSUS implementation:

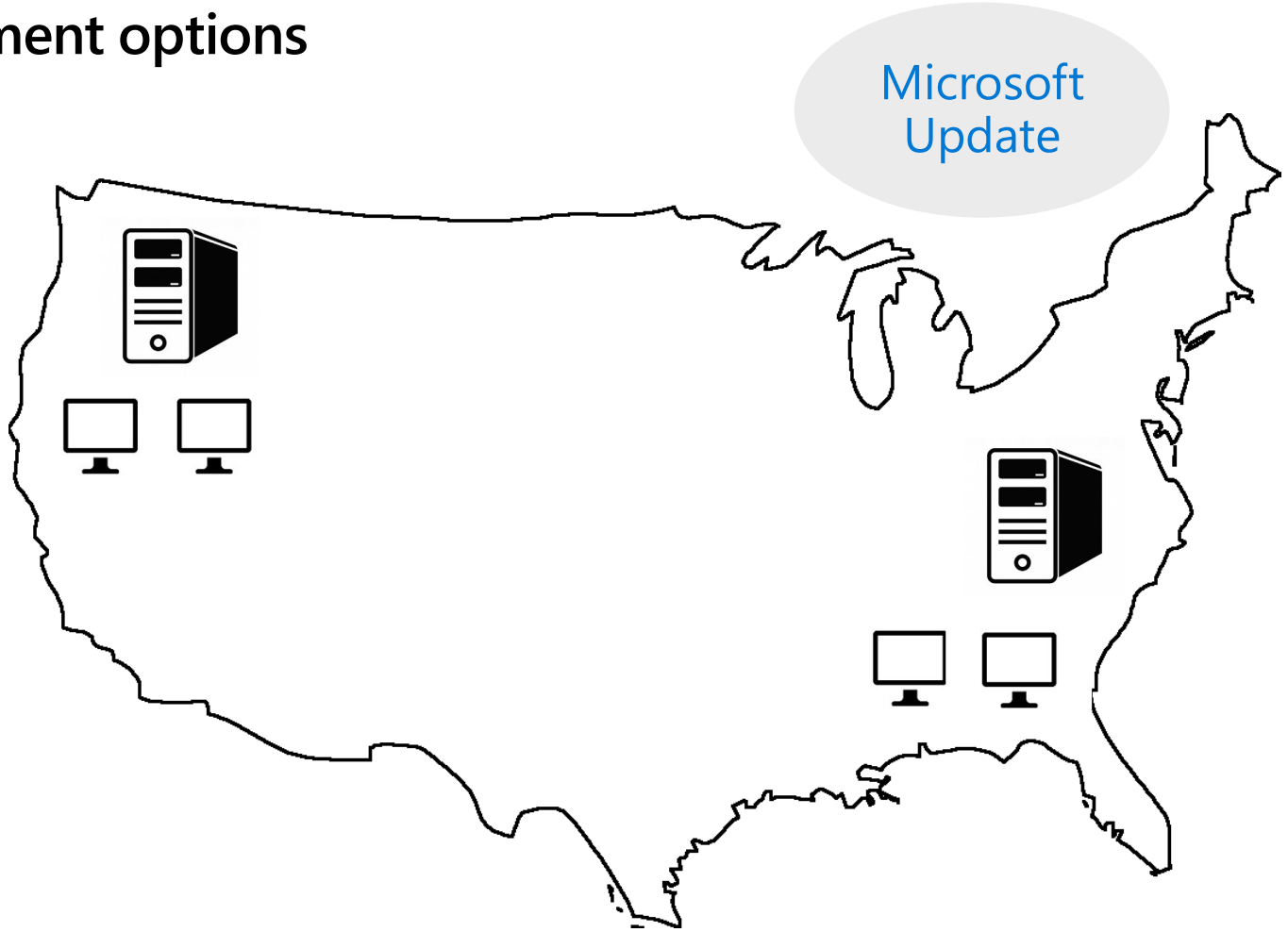
- Single server
- Multiple servers

WSUS hierarchies:

- Autonomous mode
- Replica mode

WSUS database:

- Windows Internal Database
- SQL Server database



WSUS Administration Console

You can use the WSUS Administration console to:

Manage updates

Configure computer groups

View computer status

View synchronization information

Configure and view WSUS reports

Configure WSUS settings and options

Computer Groups

You can use computer groups to organize
WSUS clients
The default computer groups include:

All computers

Unassigned computers

You can create custom computer groups to control how updates are applied

Managing Updates

Updates can be:

Approved automatically, but it is not recommended

Declined if they are not needed

Removed if they cause problems

Updates should be tested before they are approved for production

Configuring Clients to use WSUS

Use a GPO to:

Configure automatic updates

Specify intranet Microsoft update service location

To use Automatic Maintenance for installing updates on computers running Windows 8 and Windows Server 2012 and later, configure a GPO to:

Enable automatic updates with the following option:

- **4 - Auto download and schedule the install**

Module 10:

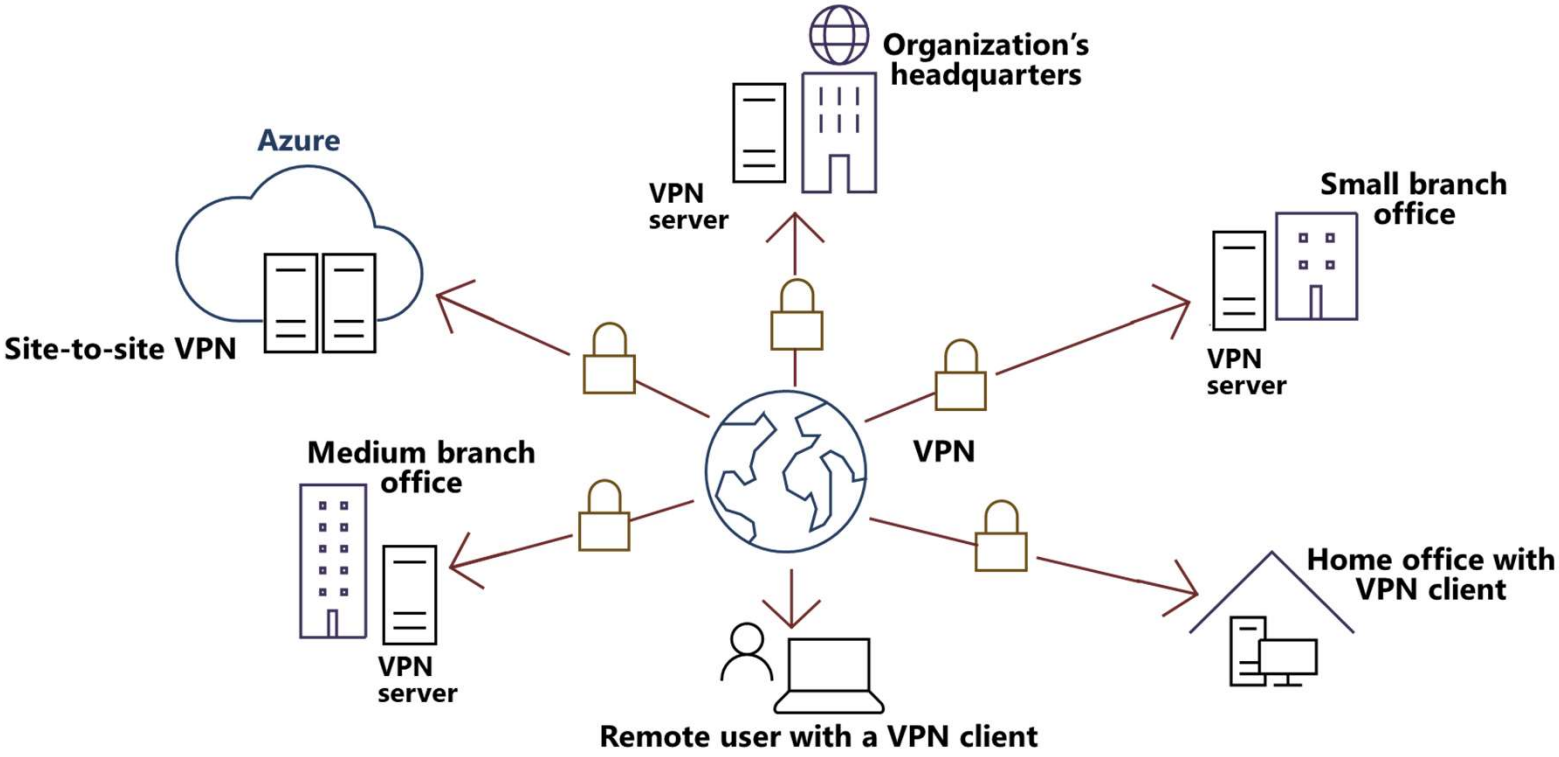
Implementing Remote Access on Windows Server 2022

Lesson 1 overview

- Topics:
  - VPN scenarios
  - Options for VPN tunneling protocols
  - VPN authentication options
  - Configure a VPN Server

VPN Scenarios

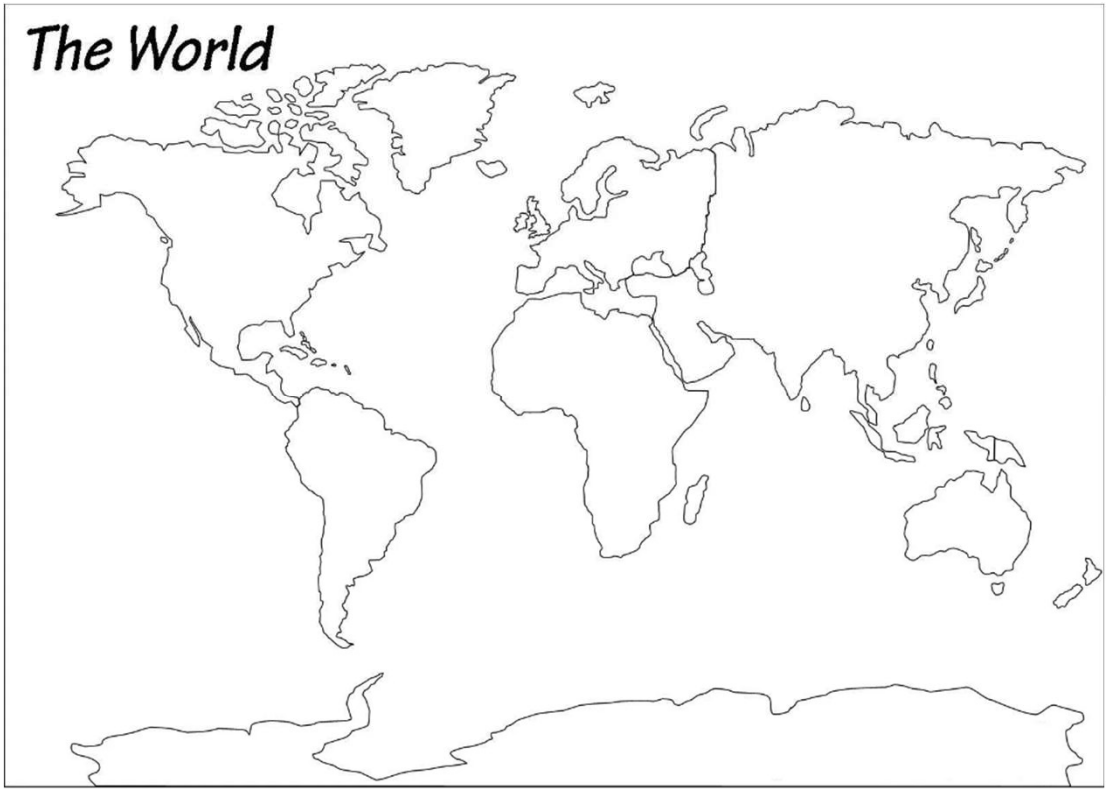
A VPN provides a point-to-point connection between a private network's components by using a public network, such as the Internet.



Options for VPN tunneling protocols

Windows Server supports four VPN tunneling protocols.

Tunneling protocol	Firewall access
PPTP	TCP port 1723
L2TP/IPsec	UDP port 500, UDP port 4500 and UDP port 1701
SSTP	TCP port 443
IKEv2	UDP port 500



VPN authentication options

Protocol	Description	Security level
PAP	Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.	The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.
CHAP	A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme.	An improvement over PAP in that the password is not sent over the PPP link. Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.
MS-CHAPv2	An upgrade of MS-CHAP. Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server to which it is dialing in to has access to the user's password.	Provides stronger security than CHAP.
EAP	Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.	Offers the strongest security by providing the most flexibility in authentication variations.

Module 11:

Managing SAN Storage and Failover Clustering

Module overview

Lessons:

- Lesson 1: ISCSI SAN
- Lesson 2: Planning for failover clustering implementation
- Lesson 3: Creating and configuring failover clusters

Lesson 1 overview

Topics:

- ISCSI SAN
- Demo: ISCSI installation and configuration

ISCSI Storage Area Networks (SAN)

RTS-DC1
192.168.1.250
ISCSI Target Server

RTS-SVR1
192.168.1.251
Access Server

RTS-SVR2
192.168.1.253
Access Server

Lesson 2 overview

Topics:

- What is failover clustering?
- High availability with failover clustering
- Failover clustering components
- Cluster quorum in Windows Server
- Considerations for planning failover clustering

What is failover clustering?

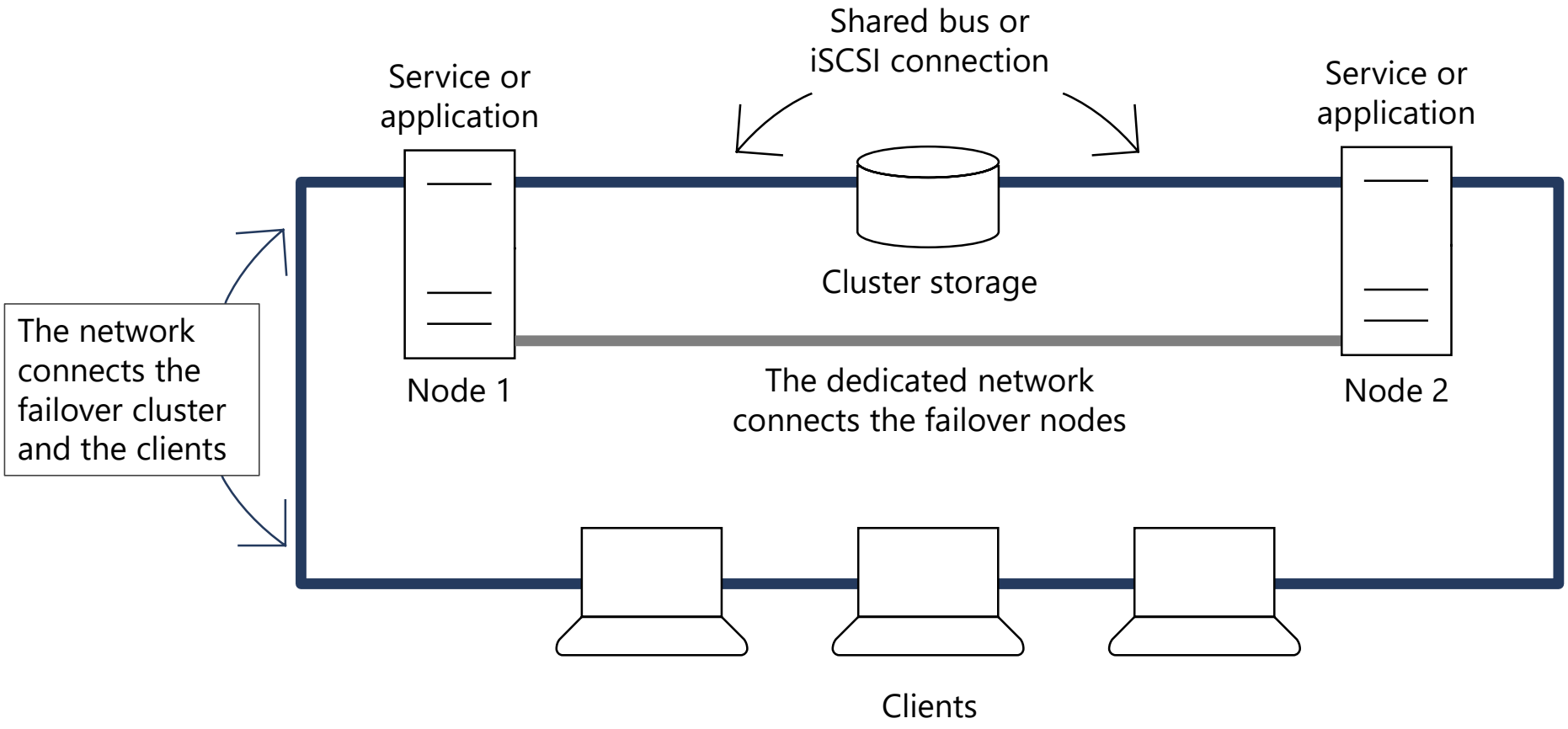
- *Failover clustering* is a group of computers that work together to increase the availability and scalability of clustered roles
- The clustered servers (called *nodes*) are connected by physical cables and by software
- If one or more of the cluster nodes fail, other nodes begin to provide service in a process known as *failover*
- Clustered roles are proactively monitored to verify that they are working properly
- If they are not working another node in the cluster runs the workload

High availability with failover clustering

Availability is a level of service expressed as a percentage of time

- *Highly available* services or systems are available more than 99 percent of the time
- Planned outages typically are not included when calculating availability

Failover clustering components

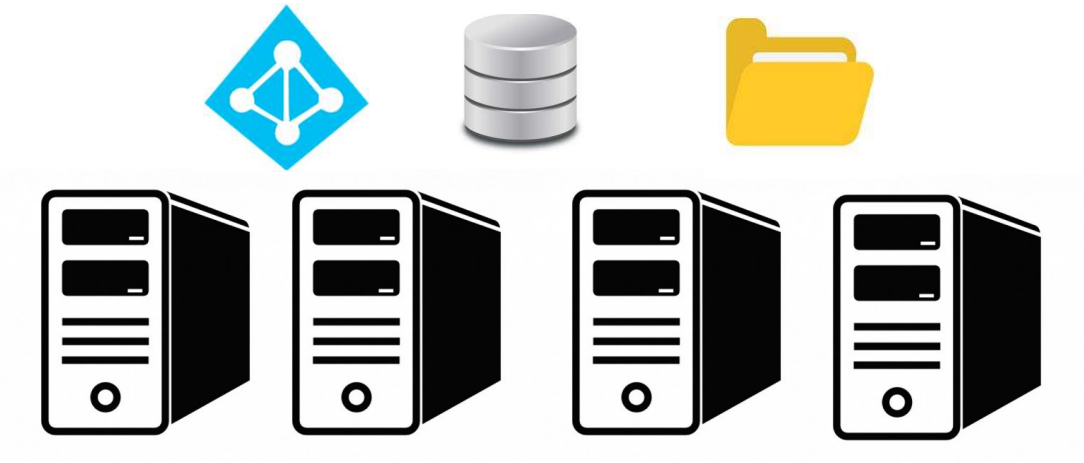


Cluster quorum in Windows Server

In failover clusters, quorum defines the consensus that enough cluster members are available to provide services.

Quorum:

- Is based on votes in Windows Server
- Enables nodes, file shares, or a shared disk to have a vote, depending on the quorum mode
- Enables the failover cluster to remain online when sufficient votes are available



Configure quorum options

Use dynamic quorum mode with:

- A disk witness
- A file share witness
- The Azure Cloud Witness

Use all other quorum modes only in specific use cases

The default and recommended best practice is to always use dynamic quorum

Lesson 3 overview

Topics:

- The Validation a Configuration Wizard and cluster support policy requirements
- Create a failover cluster
- Configure storage
- Configure networking
- Configure quorum options
- Configure roles
- Manage failover clusters
- Configure cluster properties

The Validate a Configuration Wizard and a cluster support policy requirements

The Validate a Configuration Wizard is used to perform a variety of tests to ensure the cluster components are configured in a supportable manner.

Before creating a new failover cluster, confirm the configuration to ensure all validation tests are passed.

Cluster validation is intended to:

- Ensure clustering is working properly
- Find hardware or configuration issues
- Perform diagnostic tests
- Ensure requirements for:
  - Hardware
  - Network/Infrastructure
  - Software

Create a failover cluster

To create a failover cluster, you'll need to:

- Verify the prerequisites
- Install the Failover Clustering feature on each node
- Run the Validate a Configuration Wizard
- Create the cluster using:
  - The Create Cluster Wizard, or
  - Windows Admin Center
- Create clustered roles

Configure storage

Failover clusters require shared storage to provide consistent data to a virtual server after a failover

Shared storage options include:

- SAS
- iSCSI
- Fibre Channel
- Shared **.vhdx**

Clustered storage spaces can also be implemented to achieve high availability at the storage level

Configure networking

To configure networking:

- The network hardware must be compatible with Windows Server
- In the network infrastructure that connects your cluster nodes, avoid having single points of failure

Configure roles

To configure roles:

1. Install the Failover Clustering feature
2. Verify the configuration
3. Create a cluster
4. Install the role on all cluster nodes by using Server Manager
5. Create a clustered application by using the Failover Clustering Management snap-in
6. Configure the application
7. Test the failover

Manage failover clusters

To manage failover clusters:

- Add nodes after you create a cluster
- Pause nodes, which prevent resources from running on that node
- Evict nodes from a cluster, which removes the node from the cluster configuration

These actions are available in the **Failover Cluster Management Console**, in the **Actions** pane

Configure failover and failback

To control how the cluster responds, adjust the failover and failback settings.

Include preferred owners

Considerations for using preferred owners:

- Set preferred owners are set on the clustered role
- Set multiple preferred owners can be set in an ordered list
- Setting preferred owners gives control over:
  - The order in which a role selects a node to run
  - The roles that can be run on the same nodes
- Options to modify failover and failback settings:
  - Setting the number of times the Cluster service restarts a clustered role in a set period
  - Setting or preventing failback of the clustered role to the preferred node when it becomes available

Module 12:

Performance Monitoring in Windows Server 2022

Module Overview

Overview of Windows Server monitoring tools

Using Performance Monitor

Monitoring event logs for troubleshooting

Lesson 1: Overview

Overview of Task Manager

Overview of Resource Monitor

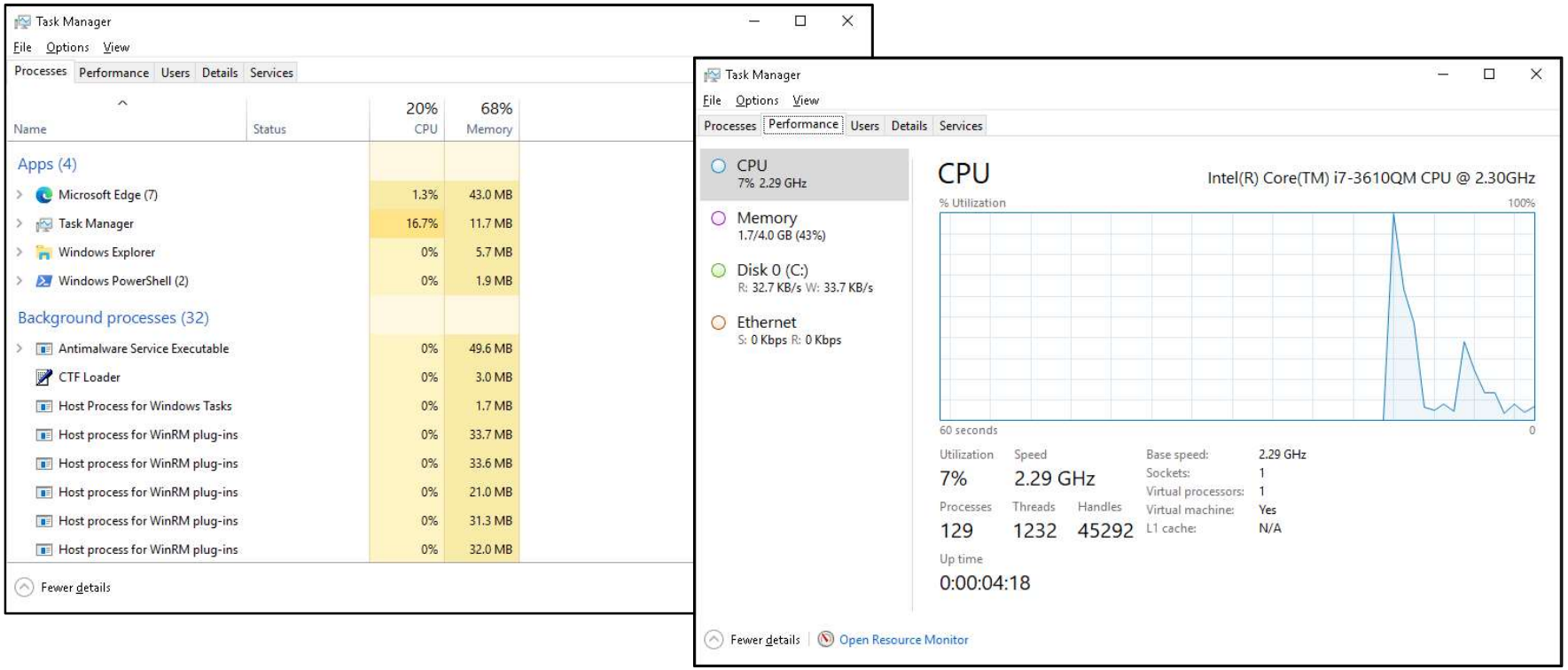
Overview of Performance Monitor

Overview of Reliability Monitor

Overview of Event Viewer

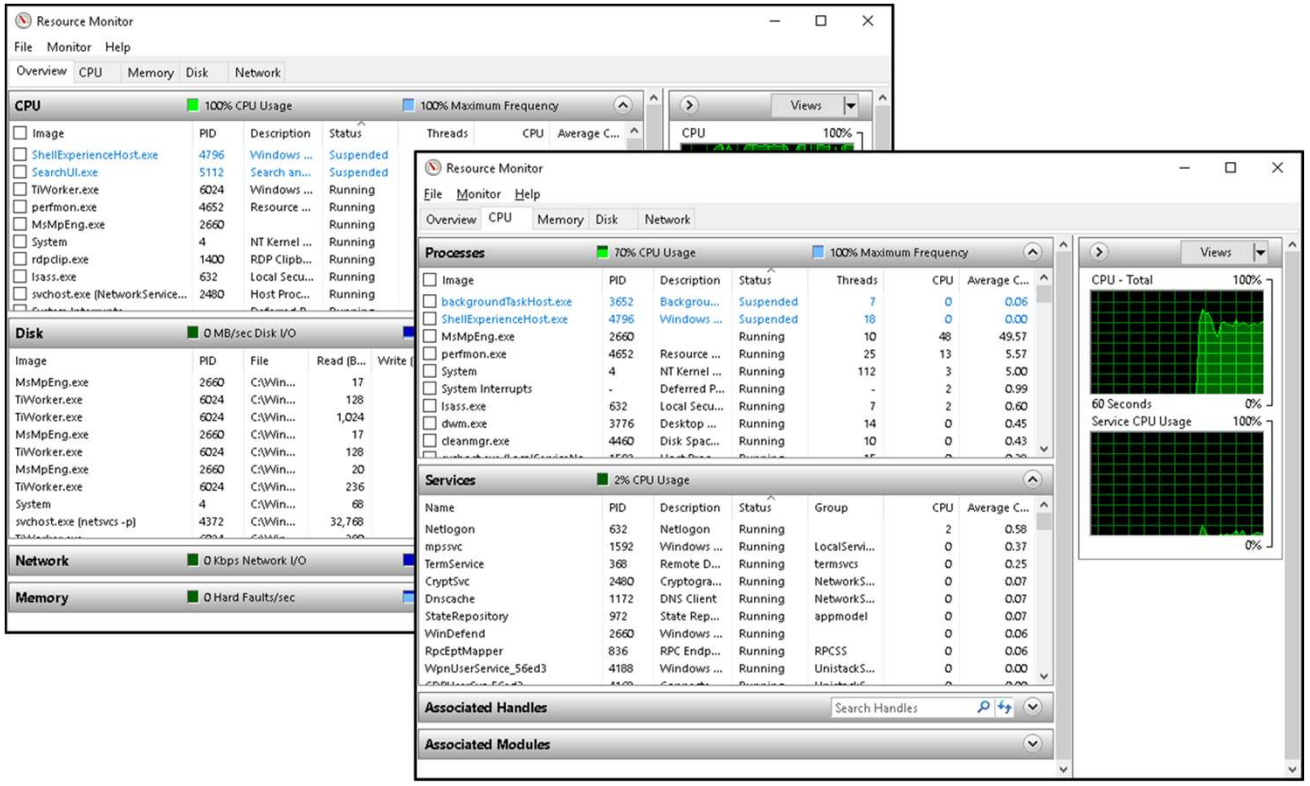
Overview of Task Manager

Task Manager helps you to identify and resolve performance-related issues



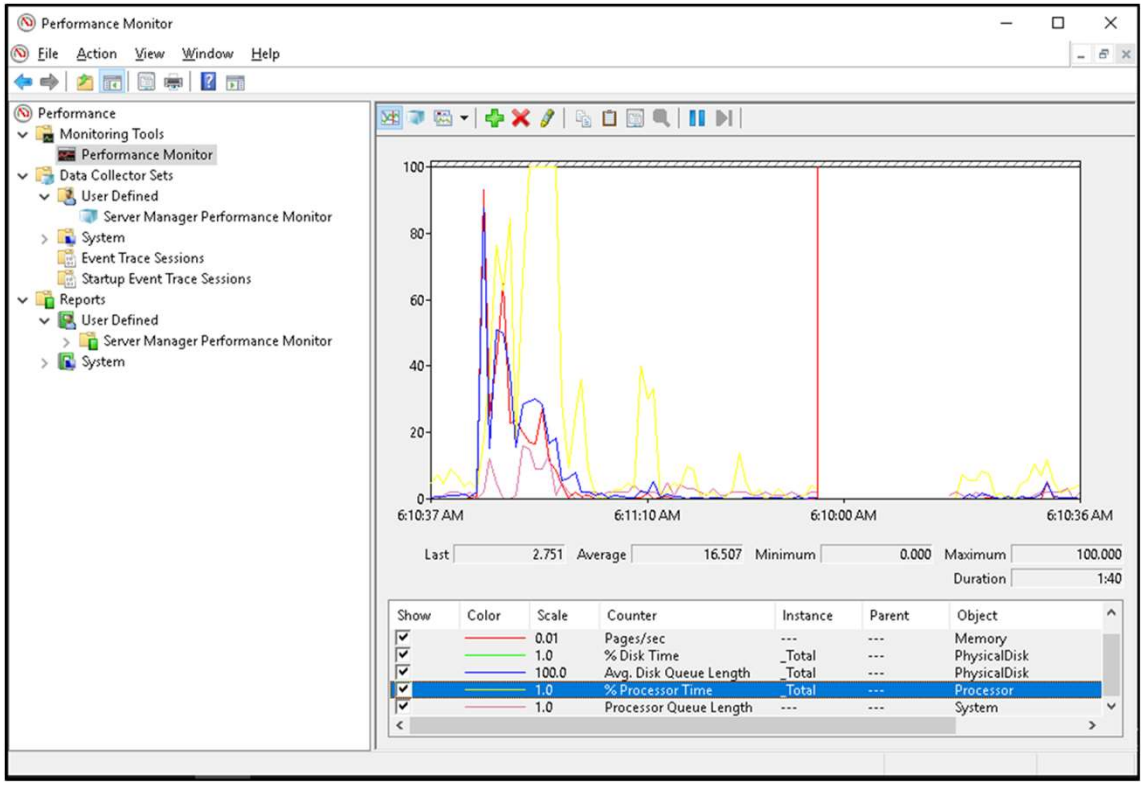
Overview of Resource Monitor

Resource Monitor provides an in-depth understanding at the real-time performance of your server



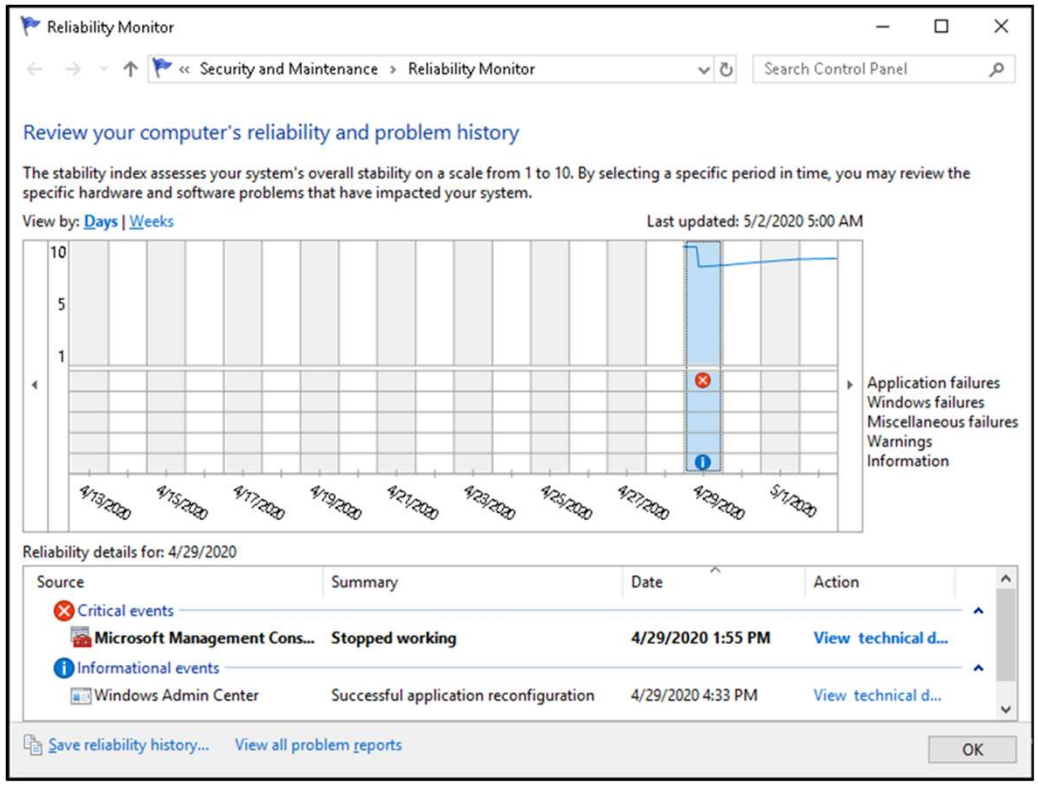
Overview of Performance Monitor

Performance Monitor enables you to observe current performance statistics or to study historical data that Data Collector Sets have gathered



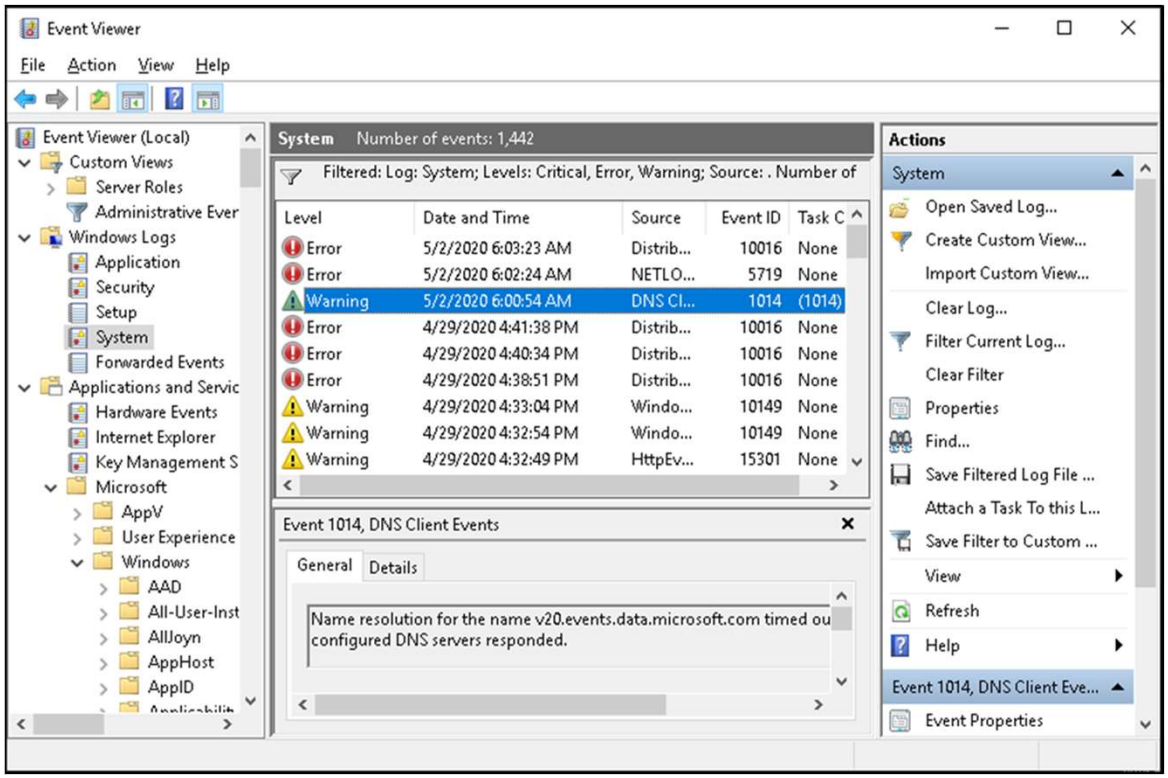
Overview of Reliability Monitor

Reliability Monitor monitors hardware and software issues that occur during the selected time interval and assigns a number called the stability index that indicates the server's reliability



Overview of Event Viewer

Event Viewer provides categorized lists of essential Windows log events and log groupings for individual installed applications and specific Windows component categories



Bonus Module:
Microsoft Azure

Lesson Overview

In this lesson, you'll learn about Azure and Microsoft Entra ID

- Topics
  - What is Azure?
  - Understanding Microsoft Entra ID (formerly Azure Active Directory)
  - Microsoft Entra ID versus Active Directory Domain Services (AD DS)
  - What is Microsoft Entra ID Connect?

What is Azure?

Azure is a cloud computing platform provided by Microsoft that offers a wide range of services to help individuals and businesses build, deploy, and manage their applications and services.

Think of Azure as a collection of powerful tools and resources that are available to you over the internet. Instead of buying and maintaining your own servers and infrastructure, Azure allows you to use Microsoft's infrastructure and services to run your applications and store your data.

Here are a few key aspects of Azure:

- **Scalability**:
- **Storage and Backup**:
- **Virtual Machines**:
- **Web and Mobile Apps**
- **AI and Machine Learning**
- **Security and Compliance**

Overall, Azure simplifies the process of building, deploying, and managing applications by providing a comprehensive set of services that are accessible over the internet. It helps you focus on your core business objectives without worrying about the underlying IT infrastructure.

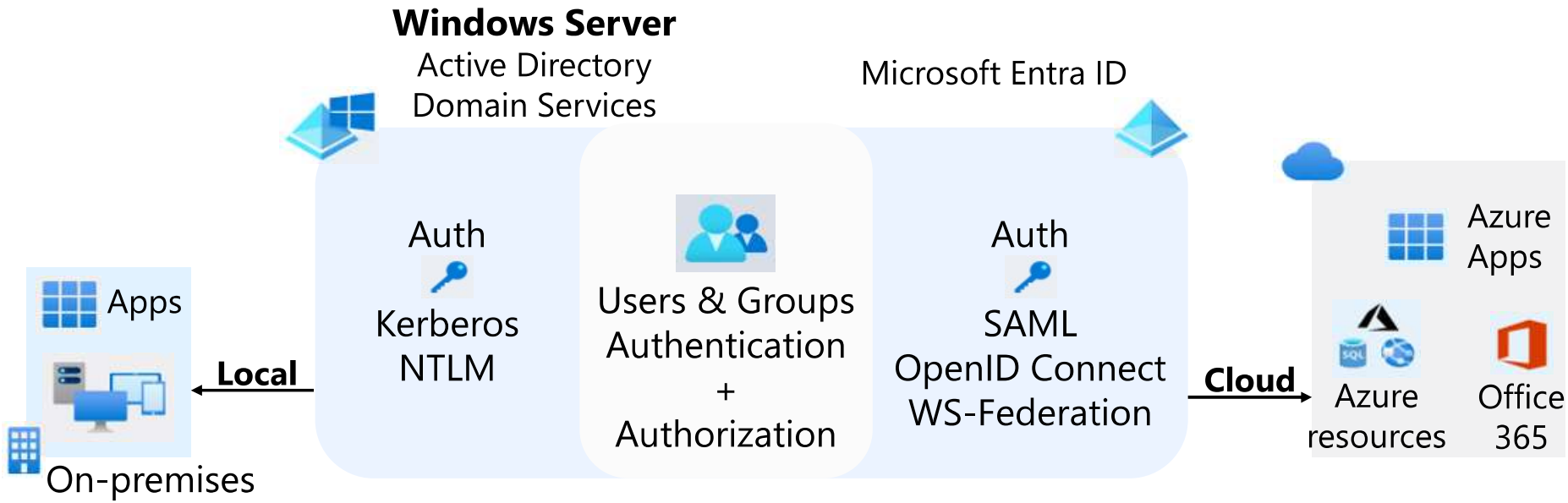
Understanding Microsoft Entra ID?

Microsoft Entra ID is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

•External resources, such as Office 365 and thousands of other applications.

•Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

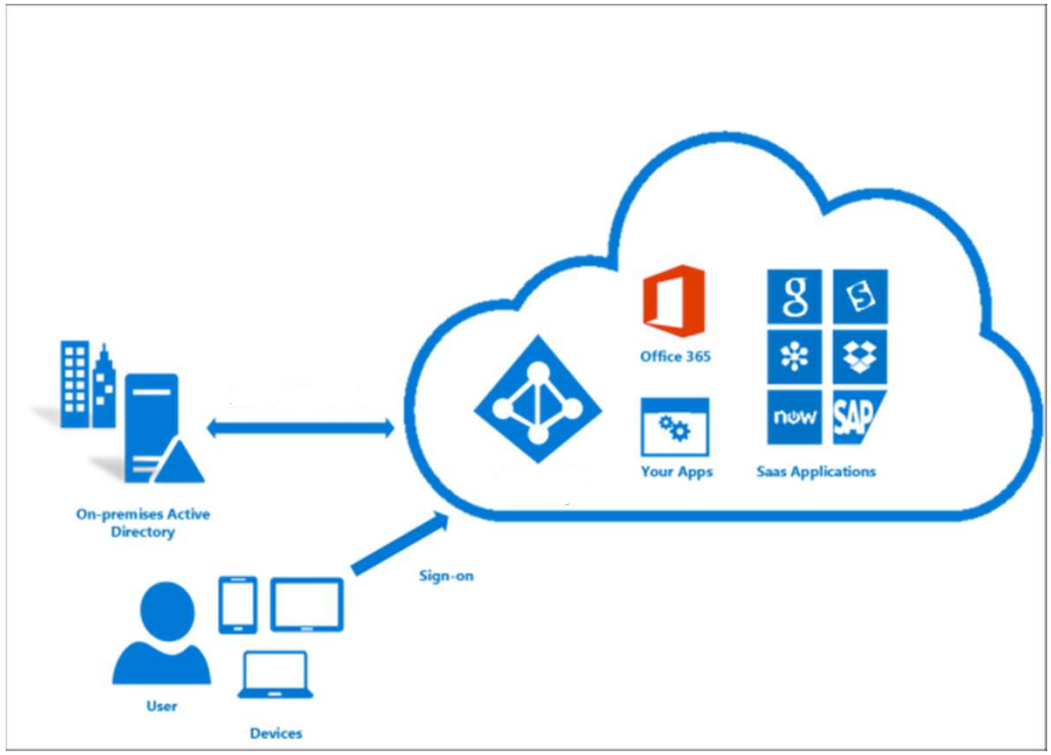
Microsoft Entra ID versus Active Directory Domain Services (AD DS)



Service	Authentication	Structure	What it's used for
Microsoft Entra ID	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM	Forests, domains, organizational units	Authentication and authorization for on-premises printers, applications, file services, and more

What is Microsoft Entra Connect?

Microsoft Entra Connect is the Microsoft tool that allows accounts from your Active Directory Domain Services in your on-premise environment to synchronize to Microsoft Entra ID:



Thank you for attending

- Microsoft Azure
- Microsoft 365
- Active Directory
- Group Policy
- Security
- Hyper-V
- Powershell
- Networking
- ChatGPT

Domain